SESIÓN ORDINARIA DE LA JUNTA DE GOBIERNO LOCAL DE

29 DE DICIEMBRE DE 2016.

ALCALDE-PRESIDENTE

Excmo. Sr. D. José López Martínez (MC).

CONCEJALES ASISTENTES

Dª Ana Belén Castejón Hernández (PSOE)
D. Juan Pedro Torralba Villada (PSOE)
D. Francisco José Calderón Sánchez (MC)
D. Ricardo Segado García (MC)

CONCEJAL SECRETARIO

D. Francisco Aznar García (PSOE)

En Cartagena, siendo las nueve horas treinta minutos del día **veintinueve de diciembre de dos mil dieciséis**, se reúnen en segunda convocatoria, en la Sala de Concejales del Palacio Consistorial, los señores que al margen se relacionan, bajo la Presidencia del Exmo. Sr. Alcalde-Presidente, *D. José López Martínez*, y con la asistencia del Concejal Secretario de la Junta, *D. Francisco Aznar García*, a fin de celebrar sesión ordinaria de la Junta de Gobierno Local y tratar los asuntos que constituyen el Orden del Día, para lo cual se ha girado citación previa.

Asisten también, invitados por la Presidencia, los CONCEJALES DELEGADOS: *Dª Obdulia Gómez Bernal (PSOE), Dª Isabel García García (MC), Dª. María Josefa Soler Martínez (MC), Dª María del Carmen Martín del Amor (PSOE) y D. David Martínez Noguera (PSOE).*

Igualmente asisten, *D. Francisco Pagán Martín-Portugués,* Director de la Asesoría Jurídica Municipal, *Dª Myriam González del Valle,* Interventora General Accidental y *Dª. Encarnación Valverde Solano,* Directora Accidental de la Oficina del Gobierno Municipal.

ORDEN DEL DÍA

1º.- Lectura y aprobación, en su caso, del Acta de la sesión ordinaria celebrada el día 21 de diciembre de 2016.

2º.- Propuestas de las siguientes Áreas de Gobierno:

ÁREA DE GOBIERNO DE HACIENDA E INTERIOR

Propuestas presentadas por el Concejal Delegado del Área de Hacienda e Interior tramitadas por los siguientes Servicios:

HACIENDA

1. Generación de crédito para la XXXVI Edición del Cartagena Jazz Festival.

2. Modificación del presupuesto de 2016 para dotar los créditos necesarios para la Fundación Teatro Romano de Cartagena.

SERVICIOS ADMINISTRATIVOS GENERALES

3. Proyecto de incorporación de procedimientos de transparencia a la tramitación por vía electrónica.

4. Proyecto de incorporación de los procedimientos de Urbanismo a la tramitación por vía electrónica.

5. Proyecto de Reglamento de evidencias digitales del Excmo. Ayuntamiento de Cartagena.

6. Proyecto de Reglamento de protección de datos del Excmo. Ayuntamiento de Cartagena.

7. Aprobación de códigos de directorio dir3 para la implantación de la administración electrónica en el Ayuntamiento de Cartagena.

ÁREA DE GOBIERNO DE URBANISMO E INFRAESTRUCTURAS

Propuestas presentadas por el Alcalde Presidente tramitadas por el siguiente Servicio:

URBANISMO

8. Adquisición de finca en calle Cuatro Santos, n.º 3 y 5, calificada como equipamiento administrativo.

9. Modificación de las condiciones de pago en relación con la expropiación de las parcelas 30.1 y 30.2 incluida en el ámbito de Sistema General Viario denominado Acceso Norte.

ÁREA DE GOBIERNO DE CULTURA Y PATRIMONIO

Propuestas presentadas por el Concejal Delegado del Área de Cultura y Patrimonio tramitadas por los siguientes Servicios:

PATRIMONIO ARQUEOLÓGICO

10. Subvención a la Fundación Teatro Romano de Cartagena.

DEPORTES

11. Reconocimiento extrajudicial de créditos de facturas correspondientes a la limpieza del Estadio Municipal Cartagonova, con cargo al presupuesto municipal vigente.

12. Subvención por concesión directa a entidades deportivas de Cartagena.

3º.- Informes de los Servicios y Negociados.

- Dación de cuenta de resoluciones y otros títulos habilitantes en materia de Intervención Urbanística dictados por el Director General de Urbanismo desde el 14 al 27 de diciembre de 2016 .

4º.- Manifestaciones del Excmo. Sr. Alcalde-Presidente.

5º.- Ruegos y preguntas.

1º.- LECTURA Y APROBACIÓN, EN SU CASO, DEL ACTA DE LA SESIÓN ORDINARIA CELEBRADA EL DÍA 21 DE DICIEMBRE DE 2016.

Se dio cuenta del acta de la sesión de referencia, que fue aprobada por unanimidad y sin reparos.

2º.- Propuestas de las siguientes Áreas de Gobierno:

ÁREA DE GOBIERNO DE HACIENDA E INTERIOR

Propuestas presentadas por el Concejal Delegado del Área de Hacienda e Interior tramitadas por los siguientes Servicios:

HACIENDA

1. **GENERACIÓN DE CRÉDITO PARA LA XXXVI EDICIÓN DEL CARTAGENA JAZZ FESTIVAL.**

Con fecha 2 de diciembre se recibió escrito el Concejal Delegado de Cultura, Educación e Igualdad, en el que da cuenta de la recaudación en taquilla de la XXXVI edición del Cartagena Jazz Festival durante el mes de noviembre, cuyo importe financia los gastos de dicho festival, procede generar el correspondiente crédito presupuestario, para lo cual se acompaña copia de los ingresos de la recaudación en la tesorería municipal (DRI 2016.1.0008247.000 y 2016.1.0008356), así como el estado de ejecución de dicho concepto de ingresos.

Por ello, a la Junta de Gobierno Local, de acuerdo con lo dispuesto en los artículos 43 y 44 del Real Decreto 500/1990, de 20 de abril, que desarrolla la Ley de haciendas locales en materia presupuestaria, así como en el artículo 13 de las Bases de ejecución del presupuesto, tengo el honor de proponer la siguiente generación de crédito en el estado de gastos del presupuesto de 2016, financiada con ingresos de naturaleza no tributaria:

Estado de Gastos:

2016.07006.3340.2269909: Festival de Jazz
Importe: 13.231,07 €

Estado de Ingresos:

2016.344: Entradas a museos, exposiciones y espectáculos.
Importe: 13.231,07 €

No obstante, la Junta de Gobierno Local, con superior criterio, resolverá.= Cartagena, a 22 de diciembre de 2016.= EL CONCEJAL DELEGADO DEL ÁREA DE HACIENDA E INTERIOR.= Firmado, Francisco Aznar García, rubricado.

La Junta de Gobierno Local acuerda aprobar, por unanimidad, al anterior propuesta.

2. **MODIFICACIÓN DEL PRESUPUESTO DE 2016 PARA DOTAR LOS CRÉDITOS NECESARIOS PARA LA FUNDACIÓN TEATRO ROMANO DE CARTAGENA.**

A fin de dotar el presupuesto de créditos necesarios para que la Fundación Teatro Romano de Cartagena abone los gastos por intereses de demora generados por el vencimiento del préstamo suscrito para la recuperación del Teatro Romano, es preciso realizar una modificación de créditos en el presupuesto para 2016. Dicha modificación se efectúa con cargo a la aplicación presupuestaria 2016.07001.3361.2279947, acompañando el documento contable de retención de crédito para transferir (RC 2016.2.0026514.000).

La modificación planteada consiste en transferir crédito entre partidas de la misma área de gasto, pero con diferente nivel de vinculación jurídica, sin que la disminución que se produce en la aplicación que lo cede ocasione perturbación alguna en el normal funcionamiento del servicio.

Por ello, a la Junta de Gobierno Local, de acuerdo con lo dispuesto en el artículo 40.1 y 3 del Real Decreto 500/1990, de 20 de abril, que desarrolla la Ley de Haciendas Locales en materia presupuestaria, así como en el artículo 12 de las Bases de Ejecución del Presupuesto, redactado al amparo del apartado 2 del artículo 40 de dicho Texto Legal, tengo a bien proponer la siguiente modificación presupuestaria por el procedimiento de transferencia de créditos:

1.- APLICACIÓN PRESUPUESTARIA QUE CEDE CRÉDITOS:		**IMPORTE**
2016-07001-3361-2279947	Limpieza, control y cuidado de zonas arqueológicas	26.000,00 €
	TOTAL	**26.000,00 €**

2.- APLICACIÓN PRESUPUESTARIA QUE RECIBE CRÉDITOS:		**IMPORTE**
2016-07001-3361-784	Fundación Teatro Romano de Cartagena	26.000,00 €
	TOTAL	**26.000,00 €**

No obstante, la Junta de Gobierno Local, con superior criterio, resolverá.= Cartagena, a 23 de diciembre de 2016.= EL CONCEJAL DELEGADO DEL ÁREA DE HACIENDA E INTERIOR.= Firmado, Francisco Aznar García, rubricado.

La Junta de Gobierno Local acuerda aprobar, por unanimidad, al anterior propuesta.

SERVICIOS ADMINISTRATIVOS GENERALES

3. **PROYECTO DE INCORPORACIÓN DE PROCEDIMIENTOS DE**

TRANSPARENCIA A LA TRAMITACIÓN POR VÍA ELECTRÓNICA.

Visto lo dispuesto en los artículos 50 a 53 de la "Ordenanza Municipal de Administración Electrónica del Ayuntamiento de Cartagena" publicada en el BORM de fecha 30 de octubre de 2010, según la cual se regula el mecanismo de incorporación de trámites y procedimientos a la tramitación por vía electrónica y que con fecha de 17 de junio de 2016 se acordó en Junta de Gobierno Local el procedimiento de aprobación de las aplicaciones de gestión de expedientes y documentos electrónicos en uso y que el Decreto de fecha 22 de junio de 2016, designó a los miembros del Grupo de Proyecto para el impulso de la Administración Electrónica en el Excmo. Ayuntamiento de Cartagena, modificado por Decreto de fecha 16 de septiembre de 2016.

Visto que con fecha de noviembre de 2016 se solicitó por el Servicio de Transparencia al Grupo de Proyecto para el Impulso de la Administración Electrónica en el Excmo. Ayuntamiento de Cartagena, mediante Memoria Justificativa, la incorporación del procedimiento automatizado que se relaciona a continuación para su tramitación por vía electrónica y su inclusión en el Catálogo de Procedimientos del Excmo. Ayuntamiento de Cartagena:

- Procedimiento del Servicio de Transparencia / Acceso a la información pública.

Visto que se han emitido los informes preceptivos según artículo 51 de la Ordenanza Municipal y se ha seguido el procedimiento previsto en el citado acuerdo de Junta de Gobierno Local de fecha 17 de junio de 2016, y habiéndose realizado los correspondientes flujogramas de los citados procedimientos por parte del Grupo de Proyecto de impulso de la Administración electrónica, es por lo que, cumpliendo con los requisitos establecidos en la normativa en vigor, particularmente en el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad y su modificación según Real Decreto 951/2015, de 23 de octubre; así como el 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 y las Normas Técnicas de Interoperabilidad que lo desarrollan, y en cumplimiento de la obligación que nos exige a las Administraciones Públicas la entrada en vigor de las Leyes 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas y 40/2015, de 1 de octubre, del Régimen Jurídico del Sector Público, en el ejercicio de las competencias que tengo atribuidas, elevo a la Junta de Gobierno Local la siguiente PROPUESTA para que, previa deliberación adopte, si lo considera procedente, el siguiente **ACUERDO:**

UNICO: La aprobación del procedimiento del Servicio de Transparencia que se relaciona a continuación para su incorporación a la tramitación por vía electrónica y su inclusión, a los efectos de información a la ciudadanía, en el Catálogo de Trámites y Procedimientos electrónicos del Excmo. Ayuntamiento

de Cartagena, y publicación en la sede electrónica. Todo ello de conformidad con lo dispuesto en el artículo 53 de la Ordenanza Municipal de Administración Electrónica:

- Acceso a la información pública.

No obstante, la Junta de Gobierno Local resolverá lo que mejor proceda.= Cartagena, a 22 de diciembre de 2016.= EL CONCEJAL DELEGADO DEL ÁREA DE HACIENDA E INTERIOR.= Firmado, Francisco Aznar García, rubricado.

La Junta de Gobierno Local acuerda aprobar, por unanimidad, al anterior propuesta.

4. PROYECTO DE INCORPORACIÓN DE LOS PROCEDIMIENTOS DE URBANISMO A LA TRAMITACIÓN POR VÍA ELECTRÓNICA.

Visto lo dispuesto en los artículos 50 a 53 de la "Ordenanza Municipal de Administración Electrónica del Ayuntamiento de Cartagena" publicada en el BORM de fecha 30 de octubre de 2010, según la cual se regula el mecanismo de incorporación de trámites y procedimientos a la tramitación por vía electrónica y que con fecha de 17 de junio de 2016 se acordó en Junta de Gobierno Local el procedimiento de aprobación de las aplicaciones de gestión de expedientes y documentos electrónicos en uso y que el Decreto de fecha 22 de junio de 2016, designó a los miembros del Grupo de Proyecto para el impulso de la Administración Electrónica en el Excmo. Ayuntamiento de Cartagena, modificado por Decreto de fecha 16 de septiembre de 2016.

Visto que con fecha de diciembre de 2016 se solicitó por el Servicio de Urbanismo al Grupo de Proyecto para el Impulso de la Administración Electrónica en el Excmo. Ayuntamiento de Cartagena, mediante Memoria Justificativa, la incorporación de los procedimientos automatizados que se relacionan a continuación para su tramitación por vía electrónica y su inclusión en el Catálogo de Procedimientos del Excmo. Ayuntamiento de Cartagena:

Servicio de Organización:

- COORDINACIÓN:
    - Coordinación se Servicios – COOR
    - Informes, Estudios y Proyectos - COIN
- ORGANIZACIÓN
    - Obra Subsidiaria – COSU
    - Servicios – CSER
    - Suministros – CSUM
    - Informes – INHA
    - Servicios Generales – SEGE

- PROCEDIMIENTOS JUDICIALES
    - Contencioso – SCON
    - Fiscalía – SFIS
    - Juzgados - SJUZ

Servicio de Planeamiento:

- PLANIFICACIÓN AMBIENTAL
    - Planificación Ambiental – PLAM
    - Autorización Fitosanitarios – AFIS
- ADMINISTRATIVO DE PLANEAMIENTO
    - Informes de Planeamiento – PLIN
    - Plan General – PLPG
    - Cédulas de Urbanización – PLCU
    - Planes Parciales y Especiales – PLPP
    - Estudios de Detalle – PLED
    - Expedientes Documentales – PLDC
    - Autorización Excepcional – PLEX

Servicio Administrativo de Gestión Urbanística:

- Gestión Genérica
    - Informes de Gestión – GEIN
    - Convenios Urbanísticos – GECO
    - Permutas y Cesiones – GEPM
    - Parcelas e Inmuebles Municipales – GEEN
    - Parcelaciones y Segregaciones – GEPA
    - Informes Servicios Técnicos Gestión – GTIN
- Gestión mediante unidades:
    - Delimitaciones de Unidades - GEDU
    - Liquidaciones Definitivas – GELD
    - Incumplimiento de Obligaciones Urbanísticas – GEIO
- Expropiaciones y Patrimonio Urbanístico
    - Expropiaciones – GEEX
        - Expedientes de Justiprecio – GEEJ
        - Declaraciones de Urgente Ocupación – GEOU
- Entidades Colaboradoras
    - Asociaciones Administrativas de Propietarios – GEAA
    - Entidades de Conservación – GEEC
    - Registro de Entidades Urbanísticas Colaboradoras – REUC
- Programas y Reparcelaciones
    - Programas y Reparcelaciones – GERP

Servicio de Urbanización y Obras:

- Departamento de Proyectos de Urbanización
    - Informes de Urbanización – OUIN

    - Proyectos de Urbanización – OUPU
    - Ejecución de Obra – OUOU
- Departamento de Ejecución de Obras
    - Proyectos de Obras Ordinarias – OUOO
- Departamento Administrativo de Urbanización y Obras
    - Acción Sustitutoria - SEAS

Servicio Administrativo de Intervención Urbanística:

- Departamento de Disciplina Ambiental
    - Informes – IFUB
    - Orden de Ejecución – OJUB
    - Sancionador – SSUB
- Departamento de Disciplina Urbanística
    - Disciplina Urbanística – UBSA
    - Ruinas – SERU
    - Informe Evaluación de Edificio – SEIE
- Departamento de Licencias de Actividad
    - Comunicación Actividad – CPAC
    - Declaración Responsable de Actividad – DRAC
    - Licencias de Actividad – AACC
- Departamento de Licencias Urbanísticas
    - Comunicación Previa en Materia de Urbanismo - CPRO
    - Declaración Responsable – DRUB
    - Demolición – UDEM
    - Informes – INMA
    - Licencias Obra Mayor – UBMA
    - Resolución Única – OBAC
    - Usos Excepcionales – USEX
    - Vista de Expedientes - UBVI
- Departamento de Ocupación y Habitabilidad
    - Declaración Responsable 1ª Ocupación – DRPO
    - Declaración Responsable 2ª Ocupación – DRSO
    - Devolución de Fianza de Demolición – DFME
    - Devolución de Fianza de Obra Mayor – DFMA

Servicio de Documentación e Información:

- INFORMACIÓN URBANÍSTICA
    - Cédulas e Informes Urbanísticos – INCU
    - Atención Directa – INAD
- DOCUMENTACIÓN URBANÍSTICA
    - Informes Documentación Urbanística - OTIN
- NUEVAS TECNOLOGÍAS
    - Nuevas Tecnologías – NTEC
    - Procedimientos – PEXE

Visto no obstante, que con fecha de 7 de octubre de 2016, se dictó acuerdo de Junta de Gobierno Local, por el que se aprobó la incorporación de los procedimientos que se detallan a continuación para su tramitación por vía electrónica: comunicación previa de actividad CPAC; declaración responsable de actividad DRAC; sancionador de disciplina urbanística UBSA; informes de disciplina ambiental IFUB; órdenes de ejecución de disciplina ambiental OJUB; y sancionador de disciplina ambiental SSUB, los cuales, han sido incorporados al conjunto del total de expedientes administrativos que se tramitan en el Servicio de Urbanismo y que conforman la Memoria justificativa cuya tramitación se solicita por el citado Servicio con fecha de 22 de diciembre, y que se encuentran anteriormente relacionados.

Visto que se han emitido los informes preceptivos según artículo 51 de la Ordenanza Municipal y se ha seguido el procedimiento previsto en el citado acuerdo de Junta de Gobierno Local de fecha 17 de junio de 2016, es por lo que, cumpliendo con los requisitos establecidos en la normativa en vigor, particularmente en el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad y su modificación según Real Decreto 951/2015, de 23 de octubre; así como el 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 y las Normas Técnicas de Interoperabilidad que lo desarrollan, y en cumplimiento de la obligación que nos exige a las Administraciones Públicas la entrada en vigor de las Leyes 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas y 40/2015, de 1 de octubre, del Régimen Jurídico del Sector Público, en el ejercicio de las competencias que tengo atribuidas, elevo a la Junta de Gobierno Local la siguiente PROPUESTA para que, previa deliberación adopte, si lo considera procedente, el siguiente **ACUERDO:**

PRIMERO: La aprobación de los procedimientos del Servicio de Urbanismo relacionados en el cuerpo de la presente resolución, para su incorporación a la tramitación por vía electrónica y su inclusión, a los efectos de información a la ciudadanía, en el Catálogo de Trámites y Procedimientos electrónicos del Excmo. Ayuntamiento de Cartagena, y publicación en la sede electrónica. Todo ello de conformidad con lo dispuesto en el artículo 53 de la Ordenanza Municipal de Administración Electrónica.

SEGUNDO: Dejar sin efecto el acuerdo de Junta de Gobierno Local de fecha 7 de octubre de 2016 por el que se procedió a la incorporación de los procedimientos de comunicación previa de actividad CPAC; declaración responsable de actividad DRAC; sancionador de disciplina urbanística UBSA; informes de disciplina ambiental IFUB; órdenes de ejecución de disciplina ambiental OJUB; y sancionador de disciplina ambiental SSUB, para su tramitación por vía electrónica, para los cuales será de aplicación lo dispuesto en el presente acuerdo.

No obstante, la Junta de Gobierno Local resolverá lo que mejor proceda.= Cartagena, a 23 de diciembre de 2016.= EL CONCEJAL DELEGADO DEL ÁREA DE HACIENDA E INTERIOR.= Firmado, Francisco Aznar García, rubricado.

La Junta de Gobierno Local acuerda aprobar, por unanimidad, al anterior propuesta.

5. PROYECTO DE REGLAMENTO DE EVIDENCIAS DIGITALES DEL EXCMO. AYUNTAMIENTO DE CARTAGENA.

Con fecha de 22 de diciembre de 2016, se ha dictado informe por la Jefe de Servicios Administrativos Generales del siguiente contenido literal:

"El artículo 3.2 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, establece que: "Las Administraciones Públicas se relacionarán entre sí y con sus órganos, organismos públicos y entidades vinculados o dependientes a través de medios electrónicos, que aseguren la interoperabilidad y seguridad de los sistemas y soluciones adoptadas por cada una de ellas, garantizarán la protección de los datos de carácter personal, y facilitarán preferentemente la prestación conjunta de servicios a los interesados". Así mismo, en su artículo 156 se describe el Esquema Nacional de Interoperabilidad como: "el conjunto de criterios y recomendaciones en materia de seguridad, conservación y normalización de la información, de los formatos y de las aplicaciones que deberán ser tenidos en cuenta por las Administraciones Públicas para la toma de decisiones tecnológicas que garanticen la interoperabilidad". En el apartado 2 del citado artículo 156 se define el Esquema Nacional de Seguridad, el cual:"tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de la presente Ley, y está constituido por los principios básicos y requisitos mínimos que garanticen adecuadamente la seguridad de la información tratada".

En el sentido anteriormente expuesto, es preciso adoptar las medidas necesarias para garantizar la fiabilidad de los documentos de manera que queden reflejadas las evidencias digitales de su gestión electrónica. El artículo 5 del Real Decreto 4/2010, de 8 de enero, por el que se aprueba el Esquema Nacional de Interoperabilidad establece que: "La interoperabilidad se tendrá presente de forma integral desde la concepción de los servicios y sistemas y a lo largo de su ciclo de vida: planificación, diseño, adquisición, construcción, despliegue, explotación, publicación, conservación y acceso o interconexión con los mismos". El Esquema de Metadatos para la Gestión de Documentos Electrónicos (EMGDE), de la Dirección de Tecnologías de la Información y de las Comunicaciones del MINHAP, establece que el esquema describe los

elementos de metadatos mínimos necesarios que contribuyen a que los documentos sean auténticos, fiables, íntegros y disponibles, en un momento determinado y a lo largo del tiempo, garantizando su interoperabilidad. También describe algunos de los metadatos necesarios para la conservación a largo plazo. Por su parte, la Norma Técnica de Interoperabilidad de Política de Gestión de Documentos Electrónicos, aprobada por Resolución de fecha 28 de junio de 2012, de la Secretaría de Estado de Administraciones Públicas, establece que los procedimientos y acciones seguidos en los distintos procesos de gestión documental generarán registros con las evidencias de la correcta aplicación de dichos procedimientos atendiendo a las necesidades de cada documento y organización. Las organizaciones realizarán evaluaciones o auditorías periódicas, convenientemente documentadas, que garanticen la adecuación de la política de gestión documental y que los procesos de gestión de documentos electrónicos se realizan conforme a lo *establecido en la política. Los resultados de dichas evaluaciones serán considerados para la actualización de la política, programa de tratamiento y procesos de gestión de documentos electrónicos.*

Por otro lado, según 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, se establece que la seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema. La aplicación del Esquema Nacional de Seguridad estará presidida por este principio, que excluye cualquier actuación puntual o tratamiento coyuntural. Se prestará la máxima atención a la concienciación de las personas que intervienen en el proceso y a sus responsables jerárquicos, para que, ni la ignorancia, ni la falta de organización y coordinación, ni instrucciones inadecuadas, sean fuentes de riesgo para la seguridad. La seguridad del sistema debe contemplar los aspectos de prevención, detección y corrección, para conseguir que las amenazas sobre el mismo no se materialicen, no afecten gravemente a la información que maneja, o los servicios que se prestan. Las medidas de prevención deben eliminar o, al menos reducir, la posibilidad de que las amenazas lleguen a materializarse con perjuicio para el sistema. Estas medidas de prevención contemplarán, entre otras, la disuasión y la reducción de la exposición. Las medidas de detección estarán acompañadas de medidas de reacción, de forma que los incidentes de seguridad se atajen a tiempo. Así mismo, el artículo 34.3, relativo a Auditoría de seguridad, del Real Decreto, hace referencia a la necesidad de registrar evidencias electrónicas como traza de las acciones ejecutadas en los entornos de las administraciones. De igual modo, el Anexo II del mismo texto normativo refuerza en la práctica los métodos de recogida de tales evidencias.

En resumen, tanto las normas técnicas de interoperabilidad como las de seguridad, obligan a las administraciones a adoptar una política

adecuada de utilización de evidencias digitales como medio para asegurar la fiabilidad, conservación y trazabilidad de la gestión de los documentos electrónicos a lo largo del tiempo, por lo que se estima la necesidad de regular una norma interna de evidencias digitales en el entorno electrónico de actuación administrativa que nos obligan las Leyes 39/2015 y 40/2015 de 1 de octubre, de Procedimiento Administrativo Común de las Administraciones Públicas y de Régimen Jurídico del Sector Público."

Consta igualmente en el expediente informe Técnico de fecha 22 de diciembre d e2016.

En virtud de todo lo anteriormente expuesto, en el ejercicio de las competencias que tengo atribuidas, elevo a la Junta de Gobierno Local la siguiente PROPUESTA para que, previa deliberación adopte, si lo considera procedente, el siguiente **ACUERDO:**

UNICO: La aprobación del Proyecto de Reglamento de Evidencias digitales del Excmo. Ayuntamiento de Cartagena que se acompaña a continuación.

No obstante, la Junta de Gobierno Local resolverá lo que mejor proceda.= Cartagena, a 23 de diciembre de 2016.= EL CONCEJAL DELEGADO DEL ÁREA DE HACIENDA E INTERIOR.= Firmado, Francisco Aznar García, rubricado.

El referido Proyecto de Reglamento es del siguiente tenor literal:

REGLAMENTO DE EVIDENCIAS DIGITALES DEL EXCELENTÍSIMO AYUNTAMIENTO DE CARTAGENA

EXPOSICIÓN DE MOTIVOS

En los actuales entornos digitales se generan miles de datos de manera permanente, algunos reglados y bien conocidos; otros aleatorios, automatizados y no siempre bajo control. Todos ellos son susceptibles de constituir evidencia digital, es decir, información que puede ser utilizada a efectos de auditoría interna o, si procede, como testimonio ante un tribunal. Por ello, procede codificar adecuadamente los mecanismos para su producción, en el caso de datos reglados; para su identificación, tanto en el caso de datos reglados como no reglados; para su gestión y conservación, cuando resulte pertinente; y para el tratamiento preventivo y reactivo de los mismos, si éstos quedan puestos en un compromiso derivado, ya del propio funcionamiento habitual de los entornos digitales contemporáneos, ya de actuaciones inintencionadas o maliciosas orientadas a destruir tales datos, o al menos a cuestionar la validez de los mismos.

El legislador ha sido cuidadoso al respecto, previendo la gestión y la conservación de evidencias digitales, tanto en el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el

ámbito de la Administración Electrónica, modificado por el Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica; como en el 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. Fuera del ámbito legislativo, el Centro Criptológico Nacional ha publicado varias guías enfocadas sobre la utilización de buenas prácticas en la gestión de evidencias digitales y las organizaciones dedicadas a la publicación de normas de mercado, como la Organización Internacional de Normalización (ISO) o la Asociación Española de Normalización y Certificación (Aenor) han sido exhaustivas al respecto.

Puesto que una adecuada identificación, gestión, tratamiento y conservación de las evidencias digitales generadas por las actuales tecnologías de la información y de las comunicaciones, así como de los peligros que las acechan, resulta esencial como testimonio de los derechos y las obligaciones de las organizaciones y para la defensa de sus intereses, el Ayuntamiento de Cartagena, sobre la base de las disposiciones y normas técnicas mencionadas, se dota del pertinente mecanismo reglamentario, que debe servir para abordar del mejor modo posible esta nueva realidad que a todos nos envuelve. De manera muy precisa, dada la complejidad de la misma, el presente Reglamento toma en consideración el hecho de que la responsabilidad de la gestión de las evidencias digitales no puede recaer sólo sobre una persona, un cargo, un órgano o una unidad, por lo que, haciendo uso del principio de diferenciación funcional, articula un conjunto de equipos interdisciplinares y colaborativos, que a su vez serán objeto de aprobación reglada.

El presente Reglamento se estructura en cuatro capítulos, tres disposiciones adicionales, una disposición final, un anexo de carácter normativo y un apartado de referencias bibliográficas. El primer capítulo – Disposiciones generales – codifica el objeto y el alcance del presente Reglamento, así como sus límites y sus ámbitos subjetivos y objetivos de aplicación. De igual modo, define el concepto de evidencia digital y su tipología en el contexto del Ayuntamiento de Cartagena.

El segundo capítulo – El Esquema Institucional de Metadatos – establece la obligatoriedad del mismo, en tanto mecanismo reglado de generación de evidencias digitales, con base en el artículo 27 del "Reglamento de Política de Gestión de Documentos Electrónicos del Excelentísimo Ayuntamiento de Cartagena". También se aplica a la articulación del procedimiento para la definición de un perfil de aplicación en el Ayuntamiento del Esquema de Metadatos para la Gestión de Documentos Electrónicos (e-EMGDE) de la Administración General del Estado.

El tercer capítulo – La auditoría de seguridad – responde a lo preceptuado en el artículo 34 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, proponiendo por tanto los mecanismos que deben regir la recogida de evidencias digitales a efectos de auditoría de seguridad en el Ayuntamiento y sus entidades vinculadas o dependientes.

El cuarto capítulo – La gestión de ciberincidentes – define los mecanismos que deben estar en vigor para recolectar evidencias digitales en los supuestos de situaciones anormales, inintencionadas o maliciosas, y de ataques a los sistemas de información del Ayuntamiento. De igual modo, define los procedimientos para diseminar y conservar tales evidencias.

La Disposición Adicional Primera armoniza la auditoría de seguridad codificada en el artículo 34 del Real Decreto mencionado con la prevista 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, de 13 de diciembre, de protección de datos de carácter personal. La Disposición Adicional Segunda prevé un plan de formación para los empleados municipales. La Disposición Adicional Tercera incorpora al Glosario de Administración Electrónica reglado en la "Ordenanza Municipal de Administración Electrónica del Excmo. Ayuntamiento de Cartagena" la terminología utilizada en el presente Reglamento.

La Disposición Final identifica el procedimiento de modificación y revisión del presente Reglamento, así como su fecha de entrada en vigor.

Por último, en Anexo I, de carácter normativo, se formula el modelo de cláusula de confidencialidad que deben suscribir las personas o las organizaciones implicadas en el tratamiento de evidencias digitales.

Las referencias bibliográficas recogen los textos que se han utilizado para la redacción del presente Reglamento.

CAPÍTULO I
Disposiciones generales

Artículo 1. Objeto.

1. Es objeto del presente Reglamento definir y ordenar el modo en que se producen, gestionan y mantienen evidencias digitales en el ámbito del Ayuntamiento de Cartagena y sus entidades vinculadas o dependientes, con el fin de dejar traza identificable de todas las actuaciones que se ejecutan enentornos electrónicos, de tal modo que, de ser preciso, puedan ser utilizadas ante un tribunal o con otros fines de auditoría interna o externa.
2. Quedan fuera del alcance del presente Reglamento las prácticas para la determinación de evidencia con fines forenses, en la medida en la que no forman parte del ámbito competencial del Ayuntamiento y sus entidades vinculadas o dependientes, ello sin perjuicio del deber de cooperación con las administraciones competentes.
3. El presente Reglamento se promulga para dar satisfacción a lo previsto en el artículo 34 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, así como en los Anexos II y III del mismo. De igual modo, da satisfacción a lo previsto en el artículo 22.4 del 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 y a lo preceptuado en el artículo 2.5 del "Reglamento sobre Política de Firma y Sello Electrónicos y de Certificados del Excelentísimo Ayuntamiento de Cartagena".

Artículo 2. Ámbito de aplicación subjetivo.

El presente Reglamento será de aplicación a las entidades que integran la Administración Municipal:

a) Los órganos administrativos del Ayuntamiento de Cartagena.
b) Cualesquiera organismos públicos y entidades de derecho público vinculados al Ayuntamiento de Cartagena o dependientes del mismo.
c) Las entidades de derecho privado vinculadas al Ayuntamiento de Cartagena o dependientes del mismo, que quedarán sujetas a lo dispuesto en las normas del presente Reglamento que específicamente se refieran a las mismas y, en todo caso, cuando ejerzan potestades administrativas.

Artículo 3. Ámbito de aplicación objetivo.

El presente Reglamento se aplicará a todos aquellos servicios, productos, plataformas, procesos, dispositivos y otros canales y medios electrónicos en uso en el Ayuntamiento y sus entidades vinculadas o dependientes.

Artículo 4. Definiciones.

1. A los efectos del presente Reglamento se entiende por evidencia digital la información o los datos, almacenados o transmitidos en formato binario, y en los que se puede confiar como evidencia ante un tribunal o con fines de auditoría.
2. A los efectos del presente Reglamento, la evidencia digital puede ser de dos tipos:
    a) Evidencia generada en el curso normal de los procesos electrónicos del Ayuntamiento y sus entidades vinculadas o dependientes. Esta evidencia queda recogida en el Esquema Institucional de Metadatos previsto en el artículo 27 del "Reglamento de Política de Gestión de Documentos Electrónicos del Excelentísimo Ayuntamiento de Cartagena". La suma de todos los historiales de eventos de todas las entidades que participan en las aplicaciones, plataformas y servicios del Ayuntamiento y sus entidades vinculadas o dependientes constituye la pista de auditoría del Ayuntamiento, que tiene carácter obligatorio e inmodificable. Las aplicaciones, plataformas y servicios que no dispongan

de tal pista de auditoría habrá de adecuarse a lo dispuesto en el presente Reglamento o ser reemplazadas.

b) Evidencia generada por acontecimientos fuera de la normalidad, inintencionados o maliciosos, en el transcurso del funcionamiento del Ayuntamiento y sus entidades vinculadas o dependientes. Esta evidencia queda recogida, además de en el Esquema Institucional de Metadatos mencionado en el apartado anterior, en las pistas de auditoría de los sistemas informáticos en uso en el Ayuntamiento y sus entidades vinculadas o dependientes, en las bitácoras y los ficheros de log de los mismos, y en cualquier otro soporte o dispositivo en el que quede traza del anormal acontecimiento que debe ser auditado e investigado. Los sistemas que no recojan traza de lo acontecido habrán de adecuarse a lo dispuesto en el presente Reglamento o ser reemplazados.

CAPÍTULO II
El Esquema Institucional de Metadatos

Artículo 5. El Esquema Institucional de Metadatos.

1. El Esquema Institucional de Metadatos del Ayuntamiento de Cartagena es el instrumento de que éste se dota para generar y mantener información acerca del contenido, el contexto, la estructura, el comportamiento y la apariencia de los documentos y otros objetos digitales, a efectos de una mejor gestión de los mismos y, en consecuencia, de una recolección más detallada de evidencia acerca de las circunstancias de su producción, gestión y conservación.
2. De conformidad con lo previsto en el previsto en el artículo 27 del "Reglamento de Política de Gestión de Documentos Electrónicos del Excelentísimo Ayuntamiento de Cartagena", el Esquema Institucional de Metadatos estará basado en el Esquema de Metadatos para la Gestión de Documentos Electrónicos (e-EMGDE), de la Administración General del Estado, del cual se elaborará un perfil de aplicación de obligado cumplimiento por todas las unidades del Ayuntamiento y de sus entidades vinculadas o dependientes.
3. Los metadatos de historial de eventos de todas las entidades que pueblan los sistemas en uso en el Ayuntamiento y sus entidades vinculadas o dependientes constituyen la pista de auditoría de tales sistemas, de modo que deben permanecer inalterados y estar sujetos a especial protección.
4. De la elaboración del perfil de aplicación del Esquema Institucional de Metadatos se ocupará un grupo de trabajo compuesto por los técnicos en tecnologías de la información y de las comunicaciones propuestos por los servicios pertinentes y designados por la Alcaldía o quien tenga las competencias delegadas en materia de Administración Electrónica, y por Letrado municipal, Técnico de

Administración General y Técnico en Administración electrónica pertenecientes al Grupo de Proyecto para el Impulso de la Administración Electrónica regulado en la "Ordenanza Municipal de Administración Electrónica del Excelentísimo Ayuntamiento de Cartagena". A meros efectos informativos y con el único objeto de facilitar la redacción del perfil de aplicación por parte de dicho grupo de trabajo, será de aplicación el Esquema de Metadatos para la Gestión del Documento Electrónico de la Administración General del Estado.

5. El Esquema Institucional de Metadatos se revisará con una periodicidad al menos anual y siempre que la evolución de las tecnologías de la información y de las comunicaciones así lo aconseje.

CAPÍTULO III
La auditoría de seguridad

Artículo 6. Desarrollo y ejecución de la auditoría.

1. La auditoría debe realizarse de una forma metodológica que permita identificar claramente:
    a) El alcance y objetivo de la misma.
    b) Los recursos necesarios y apropiados para su realización.
    c) Las debidas comunicaciones con los órganos del Ayuntamiento y de sus entidades vinculadas o dependientes que soliciten la auditoría, si ésta no se lleva a cabo de oficio.
    d) La planificación preliminar o los requisitos de información previos al desarrollo del programa de auditoría, y a la ejecución de las pruebas que se consideren necesarias.
    e) El establecimiento de un programa detallado de auditoría con las revisiones y pruebas de auditoría previstas.
    f) La presentación de los resultados individuales de las pruebas a las personas involucradas en estos resultados, para su confirmación sin valoraciones con respecto a los resultados finales.
    g) La evaluación global de los resultados de la auditoría en relación al objetivo y alcance definidos y a los requisitos 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.
    h) La confección, presentación y emisión formal del Informe de Auditoría.
2. La metodología aplicada debe permitir comprobar, a través de los registros y evidencias de auditoría, la consecución de estos pasos, las limitaciones que se hayan podido producir en el desarrollo de las tareas, y las actividades realizadas.
3. Para una consecución eficaz de la auditoría, el equipo auditor verificará que las medidas de seguridad para el sistema auditado

se ajustan a lo preceptuado en los artículos 4 y 11 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.

Artículo 7. Definición del alcance y objetivo de la auditoría.

1. El alcance y el objetivo de la auditoría deben estar claramente definidos, documentados y consensuados entre el equipo auditor y el órgano del Ayuntamiento o de sus entidades vinculadas o dependientes que la haya solicitado, si ésta no se lleva a cabo de oficio.
2. Habida cuenta de que las redes de comunicaciones y sistemas del Ayuntamiento y sus entidades vinculadas o dependientes tienen interconexiones con entidades públicas y privadas, debe definirse claramente el alcance de la auditoría y el límite de la misma.
3. Como parte de la definición del alcance de la auditoría, deben identificarse los elementos organizativos, físicos y lógicos que abarca, incluidos:
    a) Política de Seguridad.
    b) Valoración de la información y los servicios, junto con la determinación de la categoría del sistema.
    c) Política de Firma y Sello Electrónicos y Certificados, y servicios que utilizan estas técnicas.
    d) Información, servicios y demás recursos sujetos a la auditoría.
    e) Tipo de datos que se manejan así como la normativa que les sea de aplicación.
    f) Órgano responsable y personal afectado por la auditoría.
    g) Conexiones externas con otros organismos públicos o privados.
    h) Legislación que afecta al sistema de información auditado.
4. Si existe alguna información que, por indicación del Responsable del Sistema, del Servicio o del de Seguridad, no está accesible a los auditores, y ni siquiera al Jefe del equipo de auditoría, éste debe evaluar si ello supone una limitación para realizar la auditoría. Si es así, y se decide continuar con el proceso de auditoría, esta limitación debe reflejarse en el Informe de Auditoría.
5. Para asegurar la independencia objetiva del equipo auditor, las tareas de auditoría no incluirán en ningún caso la ejecución de acciones que puedan ser consideradas como responsabilidades de consultoría o similares: implantación o modificación de software relacionado con el sistema auditado, redacción de documentos requeridos para el cumplimiento del Esquema Nacional de Seguridad, procedimientos de actuación, o posibles recomendaciones de productos concretos de software, entre otros.

Artículo 8. El equipo auditor.

1. El equipo auditor deberá estar compuesto por un equipo de profesionales - Jefe del equipo de auditoría, auditores, y expertos -

que garantice que se dispone de los conocimientos suficientes para asegurar la adecuada y ajustada realización de la auditoría.

2. El equipo de auditores deberá estar dirigido y tutelado siempre por un Jefe del equipo de auditoría, cuyas funciones principales son la supervisión de todo el proceso de auditoría, la garantía de la exactitud de los hechos, la adecuación de las recomendaciones mencionadas en el Informe de Auditoría y la preservación de las evidencias de la misma.
3. El Jefe del equipo de auditoría, responsable de gestionar las tareas de auditoría, deberá probar como mínimo:
    a) Acreditación de formación y experiencia en auditoría de sistemas de información, a través de certificaciones reconocidas a nivel nacional e internacional, o bien a través de experiencia verificable de al menos cuatro años, en auditoría de tecnologías de la información.
    b) Conocimientos de seguridad y gestión de riesgos de seguridad, mediante certificación o experiencia probada de al menos cuatro años en estos elementos.
    c) Conocimiento de los requisitos establecidos en el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
    d) Conocimientos de otra legislación aplicable relativa a la protección de datos de carácter personal, y al acceso electrónico de los ciudadanos a los servicios públicos, y del 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, entre otros.
4. El resto del equipo puede no cumplir con los requisitos definidos para el Jefe del equipo de auditoría. No obstante debe tener alguna preparación previa tanto en seguridad como en auditoría de los sistemas de información, dependiendo de, y en consonancia con, las responsabilidades asignadas. La responsabilidad de la asignación de tareas al resto del equipo, incluidos los expertos, corresponde al Ayuntamiento, o en su caso a la organización privada o pública que aporte el equipo de auditoría, previo informe del Jefe del equipo.
5. Todos los integrantes del equipo de auditoría, especialmente si son externos, y los expertos, deberán haber firmado antes de comenzar la auditoría, un acuerdo de confidencialidad conforme con el "Reglamento de Protección de Datos del Excelentísimo Ayuntamiento de Cartagena" y según modelo que figura en Anexo I, de carácter normativo, del presente Reglamento.
6. Dado el carácter interdisciplinar de la auditoría, el equipo auditor debe contar al menos con los siguientes perfiles:
    a) Un experto en tecnologías de la información y las comunicaciones.

b) Un experto con conocimientos jurídicos.
c) Un experto en Procedimiento Administrativo.
d) Un experto en administración electrónica, gestión de documentos electrónicos y conservación a largo plazo.
e) Cualquier otro que el Jefe del equipo de auditoría estime pertinente en función del sistema auditado.

7. Este equipo podrá estar compuesto por auditores internos o externos, o una combinación de ambos; pero en todo caso, es necesario cumplir con los siguientes requisitos:
   a) Si el equipo de auditoría es interno, éste deberá ofrecer garantía suficiente y demostrable de su independencia y objetividad.
   b) Si participan auditores internos y externos, se debe establecer qué equipo es responsable de la supervisión y realización de la auditoría, y de la emisión del Informe de Auditoría, y consecuentemente, de los resultados de la misma. El programa de auditoría debe establecer con claridad la responsabilidad y asignación de las funciones de cada integrante del equipo auditor.
   c) Sean auditores externos o internos, o un equipo mixto, la propiedad de los documentos de trabajo y de las evidencias, así como la responsabilidad de la emisión del Informe de Auditoría y su contenido deben ser siempre inequívocas, tanto en la apertura de la auditoría, como en su informe final. En cualquier caso, la propiedad de los documentos de trabajo y de las evidencias corresponderá al Ayuntamiento.
   d) Si la realización de la auditoría ha sido encargada a un equipo externo, privado o público, los integrantes deberán firmar las preceptivas cláusulas de confidencialidad, incluyendo las cláusulas aplicables de la legislación de protección de datos de carácter personal, de conformidad con el modelo que se incluye en el Anexo I, de carácter normativo, del presente Reglamento.
   e) Si la auditoría es liderada por un equipo de auditoría interna, pero con la incorporación de expertos independientes, éstos también deben firmar dicha cláusula de confidencialidad.
8. El equipo auditor, en el diseño de sus pruebas y revisiones, no debe limitarse a la revisión de documentos, ya que el objetivo de la auditoría es obtener evidencias eficaces para evaluar y sustentar si, en la práctica, las medidas de seguridad auditadas son adecuadas para proteger la autenticidad, fiabilidad, exactitud, integridad, identidad, completitud, disponibilidad, confidencialidad y trazabilidad de la información tratada, almacenada o transmitida por el sistema auditado. Por tanto, cualquier componente del sistema que pueda ofrecer traza de que las mencionadas propiedades de la información existen o, por el contrario, han sido

puestas en compromiso, debe ser objeto de examen y éste debe quedar documentado en el Informe de Auditoría.

Artículo 9. Planificación preliminar de la auditoría.

1. Para la realización de la auditoría es necesario realizar una planificación preliminar que consiste en establecer los requisitos de información y documentación necesarios e imprescindibles para:
    a) Establecer y desarrollar el programa de auditoría.
    b) Concretar los conocimientos necesarios del equipo de auditoría.
    c) Definir la agenda de revisiones, reuniones y entrevistas.
    d) Definir las revisiones y pruebas a realizar.
    e) Adjudicar las tareas a los componentes del equipo de auditores y expertos.
2. Si se realiza una auditoría conjunta con la requerida por los artículos 96 y 110 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, se debe identificar qué medidas de seguridad entran en el alcance de esta última.
3. La documentación mínima a requerir para concretar la planificación en detalle de la auditoría es:
    a) Documentos firmados por el órgano superior correspondiente que muestren el conocimiento y la aprobación formal de las decisiones en materia de política de seguridad.
    b) Organigrama de los servicios o áreas afectadas, con descripción de funciones y responsabilidades.
    c) Identificación de los responsables de la información, de los servicios, de la seguridad y del sistema.
    d) Descripción detallada del sistema de información a auditar: software, hardware, comunicaciones, equipamiento auxiliar, ubicaciones y similares.
    e) Identificación de la categoría del sistema según el Anexo I 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.
    f) Niveles de seguridad definidos.
    g) Política de Seguridad.
    h) Política de Firma y Sello Electrónicos y de Certificados de la Administración, si se emplean estas tecnologías.
    i) Normativa de seguridad.
    j) Descripción detallada del sistema de gestión de la seguridad y la documentación que lo sustancia.
    k) Informes de análisis de riesgos.
    l) Declaración de Aplicabilidad.
    m) Decisiones adoptadas para gestionar los riesgos.
    n) Relación de las medidas de seguridad implantadas.

o) Relación de registros de actividad en lo relativo a las medidas de seguridad implantadas.
p) Informes de otras auditorías previas de seguridad relacionados con los sistemas y servicios incluidos en el alcance de la auditoría, como podría ser, el informe de la auditoría bienal de protección de datos de carácter personal, o de auditorías previas con el mismo objetivo y alcance que la auditoría a comenzar.
q) Informes de seguimiento de deficiencias detectadas en auditorías previas de seguridad, y relacionadas con el sistema a auditar.
r) Lista de proveedores externos cuyos servicios se ven afectados o entran dentro del alcance de la auditoría, y evidencias del control realizado sobre estos servicios.

4. Según la disponibilidad de esta documentación, y de acuerdo con los responsables de la información, del servicio y del responsable de seguridad, el Jefe del equipo de auditoría determinará si es necesario recibir una copia, o bien, según el caso, es suficiente con una presentación de esta documentación, por parte de tales responsables.
5. En todos los casos el equipo auditor mantendrá una lista actualizada de la documentación solicitada y su situación en cuanto a si fue recibida una copia, o se permitió el acceso para su revisión.

Artículo 10. Programa de auditoría.

1. Para la planificación de la auditoría se tendrán en cuenta las siguientes premisas:
    a) Los criterios organizativos del órgano responsable del sistema auditado y la descripción de las funciones del personal afectado por este sistema.
    b) Los elementos de la seguridad que pueden auditarse mediante la revisión de documentación, observación, o entrevistas.
    c) El Documento de Seguridad previsto en el Reglamento de Protección de Datos y Documento de Seguridad del Excelentísimo Ayuntamiento de Cartagena.
    d) La selección de medidas de seguridad a verificar en cuanto a su cumplimiento tal y como han sido aprobadas.
    e) Las revisiones que deben realizarse mediante la ejecución de pruebas técnicas (accesos; visualización de registros; edición de parámetros de seguridad; observación y fotografía, si es aplicable, de las medidas de seguridad física, etc.), estableciendo muestras de elementos a revisar. Las pruebas podrán realizarse en base a muestras, pero el equipo auditor debe sustentar que la muestra de elementos seleccionada para una prueba determinada, es

suficientemente representativa, para garantizar la solvencia de los resultados.

f) Las evidencias que se espera obtener en cada prueba y cuáles son ineludibles para documentar la realización de la prueba.

g) Asignación de tareas a cada integrante del equipo de auditoría según su cualificación y experiencia, y asignación de tareas a los expertos. Deberá dejarse constancia de la supervisión de su trabajo.

2. Si existen informes recientes de auditorías previas, internas o externas, que hayan incluido la revisión de elementos afectados por la auditoría en curso, éstos podrán considerarse en la planificación y no repetir pruebas, siempre y cuando:
   a) De acuerdo a la información inicial recibida, no se hayan modificado las medidas de seguridad y se pueda tener acceso a las evidencias de las pruebas realizadas en su momento. Si las medidas se han modificado, por cualquier circunstancia, ya sea por razones de mejora continua, o para solventar deficiencias identificadas en la auditoría anterior, la medida de seguridad se volverá a revisar.
   b) Estas auditorías previas hayan tenido el grado de independencia objetiva y cualificación, similar al requerido para la realización de la auditoría prevista en el artículo 34 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.
3. Los elementos a incluir en la planificación de la auditoría, como elementos mínimos a considerar, son los siguientes, teniendo como referencia el Anexo II del Real Decreto mencionado en el apartado anterior:
   a) Análisis y gestión de riesgos, cuyos tipos de pruebas podrán ser, de manera no exhaustiva: sustentación metodológica del análisis de riesgos realizado, su coherencia y documentación, y verificación del inventario de activos. A tal fin se hará uso de una metodología contrastada a nivel nacional o internacional, de la que se dará cuenta explícita.
   b) El marco organizativo y la segregación de funciones, cuyos tipos de pruebas podrán ser, de manera no exhaustiva: documentación de las políticas y procedimientos; accesibilidad por el personal al que afecta y actualización; la comunicación de las normas, de las responsabilidades y de la concienciación del personal afectado por tales normas, y por políticas y procedimientos. A los efectos de una evaluación más representativa, se debe entrevistar no sólo a cargos jerárquicos, sino también a otro personal de forma aleatoria.

c) El marco operacional: control de accesos, explotación, servicios externos, continuidad del servicio, y monitorización del sistema, cuyos tipos de pruebas podrán ser, de manera no exhaustiva: evaluación de las pruebas fehacientes de la continuidad del servicio, con inclusión o no de los servicios externos; las autorizaciones y solicitudes de acceso, el registro y seguimiento de los incidentes de seguridad; la adecuación de los derechos de acceso que consideren la segregación de funciones, evaluación del control de capacidad de los sistemas, los mecanismos de control para el acceso físico, etc.
d) La Declaración de Aplicabilidad que recoge las medidas de seguridad del Anexo II del Real Decreto mencionado en el apartado anterior que son relevantes para el sistema de información sujeto a la auditoría, cuyos tipos de pruebas podrán ser, de manera no exhaustiva: la revisión de los registros de actividad, su revisión y supervisión; fortaleza de las medidas de seguridad de las comunicaciones frente a ataques internos o externos, control de cambios en aplicaciones y sistemas, cumplimiento de contratos de propiedad intelectual, etc.
e) Los procesos de mejora continuada de la seguridad, cuyos tipos de prueba podrán ser, de manera no exhaustiva: evaluación del ciclo de madurez del sistema de gestión de la seguridad del sistema de información auditado, criterios para la revisión y agenda de mejoras.
f) La aplicación de los modelos de cláusula administrativa particular a incluir en las prescripciones administrativas de los contratos correspondientes, de conformidad con lo previsto en el Anexo V del Real Decreto mencionado en el apartado anterior y en la Disposición adicional segunda de la Ordenanza Municipal de Administración Electrónica del Excelentísimo Ayuntamiento de Cartagena, según una muestra seleccionada de éstos.

4. Para definir la tipología de pruebas a realizar, el equipo auditor podrá utilizar guías y cuestionarios de auditoría disponibles en asociaciones y colectivos de auditores, y las guías STIC proporcionadas por el Centro Criptológico Nacional que sean de aplicación al sistema auditado.
5. El Jefe del equipo auditor debe valorar qué información o documentación es necesaria solicitar al comienzo de la auditoría, para asegurar que se tiene una fotografía fiel de determinadas medidas de seguridad al comienzo de la misma, como pueden ser, entre otros posibles y según se considere aplicable:
    a) Lista del personal que ha dejado el organismo recientemente.
    b) Copia del registro de incidencias.
    c) Copia del registro de actividad de los usuarios.

d) Registros de formación del personal afectado por el sistema auditado.

6. Durante la definición de las pruebas a realizar, se valorará si es necesario solicitar cuentas de acceso al sistema auditado para algunos integrantes del equipo auditor.

Artículo 11. Revisiones y pruebas de auditoría.

1. Para la realización de las pruebas de auditoría, el auditor tendrá en cuenta como normas generales, las siguientes premisas:
   a) La planificación de las pruebas a realizar, especialmente las de observación y pruebas técnicas, es un elemento privativo del equipo auditor. Por lo tanto, éste no tiene obligación de anticiparlas al personal auditado, excepto en lo que concierne a la agenda o disponibilidad de elementos para la ejecución de la prueba.
   b) En la realización de determinadas pruebas como la verificación documental de autorizaciones, aprobaciones o contratos, el auditor podrá requerir la revisión de los documentos. Estos documentos, bien en soporte electrónico o en papel, podrán ser originales o constituir alguno de los tipos de copia previstos en la 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 Procedimientos de copiado auténtico y conversión entre documentos electrónicos, en relación a la evidencia a la que deban servir a efectos de verificación.
   c) La muestra seleccionada de medidas o documentación debe ser suficiente y relevante para satisfacer el cumplimiento objetivo de la prueba, dentro del alcance y objetivo de la auditoría. El Jefe del equipo de auditoría puede decidir que se amplíe la muestra si considera que el tamaño de ésta no es suficiente.
   d) El equipo auditor no prejuzgará, a priori, en la existencia de determinadas medidas, ni será inflexible en su funcionalidad. Al evaluar las medidas existentes deberá siempre considerar, objetivamente, si se ajustan a lo previsto en el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica y si previenen realmente los riesgos identificados en el análisis de riesgos.
   e) Ante la ausencia de determinada medida, se investigará y analizará si existen otras medidas compensatorias, y en su caso, se evaluará la eficacia de estas últimas.
   f) Las entrevistas no se plantearán de forma inductiva, sino abierta. Es decir, no se deben realizar preguntas donde la respuesta, afirmativa o negativa según el caso, esté implícita en la pregunta.

g) Se ponderarán las respuestas de las entrevistas, pudiendo haber lugar a la realización de pruebas complementarias que no estaban previstas.

2. Para las evidencias de las pruebas el auditor tendrá en cuenta como normas generales, las siguientes:
   a) El Jefe del equipo auditor deberá supervisar todo el trabajo realizado y comprobar que se ha llevado a cabo el programa de auditoría previsto y aprobado, y que las desviaciones al programa, o sus modificaciones, están debidamente fundamentadas, y registradas.
   b) La evidencia recogida debe ser suficiente y relevante para que, si no hay incidencias a comunicar, se acredite la realización adecuada de la prueba y sus resultados; o, si hay incidencias a incluir en el informe, se sustente claramente el incumplimiento persistente o una indiscutible deficiencia de seguridad, y no situaciones excepcionales o puntuales, si están reportadas, controladas, y aprobadas, a menos que la excepcionalidad no debiera haber sido aprobada, por el riesgo que pudiera implicar, según el juicio objetivo y sustentado del auditor.
   c) La revisión de documentación, incluido el análisis de riesgos, deberá documentarse con las conclusiones de la revisión, y las posibles aclaraciones recibidas posteriormente.
   d) Las conclusiones, o la información recogida en una entrevista, para poder ser considerada como evidencias de auditoría, deberá ser plasmada en actas comunicadas a las personas entrevistadas.
   e) Los correos electrónicos, en la medida que involucren a varias personas dentro del alcance de la auditoría, y se disponga del acuse de recibo, podrán servir, en determinados casos, como prueba de auditoría, previa autorización del titular de la cuenta o mediando orden judicial.
   f) Las pruebas de observación, como las de seguridad física, deberán estar documentadas ya sea a través de fotografías, documentación similar, o comunicaciones escritas puntuales al Responsable de Seguridad.
   g) Las evidencias que se recojan deben evitar, en lo posible, contener datos de carácter personal, o si es necesario como evidencia que los contengan, debe utilizarse algún mecanismo (supresión, tachado, etc.) que impida su divulgación.
   h) Las evidencias que haya que presentar a requerimiento de quien tenga competencias para solicitarlas, deberán acogerse a la práctica habitual y en particular, si se trata de evidencias digitales, deberán someterse a las Normas Técnicas de Interoperabilidad que resulten de aplicación.
   i) Los documentos de trabajo del auditor (planificación, documentación revisada, evidencias, actas de reuniones,

listados, copias de pantallas, y evidencias similares del trabajo realizado, ya sean en soporte papel o electrónico) deberán mantenerse de manera permanente, debidamente referenciados y archivados, así como custodiados y protegidos en el archivo electrónico único del Ayuntamiento.

Artículo 12. Elaboración y presentación de los resultados de revisiones y pruebas de auditoría.

1. El objetivo principal de la presentación de los resultados de las revisiones y pruebas, antes de la emisión del Informe de Auditoría, es confirmar los hechos y las situaciones detectadas o identificadas como resultado de las pruebas y revisiones realizadas. Esta presentación tendrá un carácter aséptico, sin valoraciones subjetivas, ni aludiendo a la valoración de los resultados finales a plasmar en el informe, que es la opinión profesional del auditor.
2. Todos los resultados de pruebas, relacionados entre sí o que se refieran a una misma deficiencia o debilidad, serán agrupados para el informe, aun cuando se incluya un detalle de las deficiencias de forma individual, en un anexo al Informe de Auditoría.
3. En relación con los requisitos del Título VIII del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, cuando haya una divergencia contrastable entre la aplicación de éstos y los 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, resultando un incumplimiento del primero, se debe indicar con claridad esta situación, ya que los requisitos del Real Decreto 1720/2007 son prioritarios, en la medida en la que desarrollan una ley orgánica.
4. Si bien el objetivo principal es la verificación del cumplimiento aceptable del Real Decreto 3/2010 mencionado en el apartado anterior, el equipo auditor deberá tener en cuenta que estos requisitos son mínimos y por lo tanto, si observara alguna deficiencia que puede implicar riesgos en la protección de la información, como las identificadas en el Capítulo IV del presente Reglamento, deberá comunicarlo.

Artículo 13. Presentación del Informe de Auditoría.

1. Una vez confirmados los hechos y deficiencias resultado de las revisiones y pruebas de auditoría, deberá presentarse un Informe de Auditoría al Responsable del Sistema y al Responsable de Seguridad. Los informes de auditoría serán analizados por el responsable de seguridad competente, que elevará las conclusiones al responsable del sistema para que adopte las medidas correctoras adecuadas.

2. El equipo auditor no entregará ni concederá acceso al Informe de Auditoría a terceros distintos de los indicados en el párrafo anterior, salvo por imperativo legal o mandato judicial.
3. El Informe de Auditoría deberá dictaminar sobre la adecuación de las medidas exigidas por el Real Decreto 3/2010 mencionado en el artículo anterior, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias. Deberá, igualmente, incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y las recomendaciones propuestas.
4. El informe incluirá las no conformidades encontradas durante la realización de la auditoría.
5. El informe incluirá una opinión acerca de si:
    a) La Política de Seguridad define los roles y funciones de los responsables de la información, los servicios, los activos y la seguridad del sistema de información.
    b) Existen procedimientos para la resolución de conflictos entre dichos responsables.
    c) Se han designado personas para dichos roles a la luz del principio de separación de funciones.
    d) Existe un sistema de gestión de la seguridad de la información, documentado y con un proceso regular de aprobación por la dirección.
    e) Se ha realizado un análisis de riesgos, con revisión y aprobación regular, según lo establecido en las medidas aplicables del Anexo II del Real Decreto 3/2010 mencionado en el artículo anterior.
    f) Se cumplen las medidas de seguridad descritas en el citado Anexo II, sobre Medidas de Seguridad, en función de las condiciones de aplicación en cada caso.
    g) Existe un sistema de gestión de mejora continua.
6. Si la auditoría se realizara conjuntamente con la requerida por los artículos 96 y 110 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, es necesario que el Informe indique con claridad cuándo una deficiencia de seguridad o incumplimiento, o una mejora recomendada está, individualmente, relacionada con ambas normas, o bien con una en concreto.
7. El Informe de Auditoría se podrá presentar en formato audiovisual. No obstante, este Informe siempre deberá entregarse en soporte electrónico y debidamente firmado. El esquema del Informe incluirá como mínimo:
    a) Fecha de emisión del informe.
    b) Una sección de alcance, limitaciones al alcance, y objetivo de la auditoría, con la debida identificación del sistema auditado.

c) Breve descripción del proceso metodológico aplicado para realizar la auditoría.
d) Identificación de la documentación revisada.
e) Identificación de la tipología de pruebas realizadas.
f) Las fechas de comienzo y final del trabajo de campo, ya sean reuniones o revisiones técnicas, realizado durante el proceso de auditoría.
g) Indicación de si ha habido alguna limitación en la realización de las pruebas o revisiones, que impidan dar una opinión sobre determinados elementos de seguridad.
h) Una sección de informe ejecutivo resumiendo los aspectos más relevantes o las áreas de acción más significativas, con un resumen general del grado de cumplimiento.

8. Las recomendaciones en ningún caso deberán ser cerradas, sino sugerencias de las distintas alternativas posibles, cuando sea aplicable, a considerar por los responsables de seguridad.
9. Las recomendaciones estarán siempre basadas en la existencia de un riesgo y sustentadas debidamente, o bien relacionadas con un incumplimiento fehaciente y preciso de los requisitos básicos y mínimos 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. En anexos se podrán describir los detalles y resultados de las pruebas que permiten llegar a las conclusiones del informe ejecutivo, agrupándolos por los apartados del informe ejecutivo.
10. El Informe también podrá incluir como anexo las contestaciones del Responsable de Seguridad a los comentarios vertidos en el informe, o las acciones que se tomarán para solucionar las deficiencias, si las hubiera.
11. El Informe de Auditoría deberá ser firmado por el Jefe del equipo de auditoría, e indicar los participantes en el equipo de auditoría en un anexo o a continuación de la firma del Jefe del equipo.
12. En el informe ejecutivo no se incluirán términos o acrónimos informáticos, ya que el informe podrá ser leído por personas que no tengan el conocimiento informático adecuado. Tampoco se deberán incluir nombres de personas concretas, sólo funciones o puestos desempeñados.

CAPÍTULO IV
La gestión de ciberincidentes

Artículo 14. Definición de ciberincidente.

A los efectos del presente Reglamento, se entiende por ciberincidente toda acción desarrollada a través del uso de redes de ordenadores u otros medios, que se traducen en un efecto real o potencialmente adverso sobre un sistema de información, la propia información que trata o los servicios que presta. Se trata, por tanto, de un incidente relacionado con la

seguridad de las Tecnologías de la Información y las Comunicaciones que se produce en el Ciberespacio. Sin ánimo de exhaustividad, pueden considerarse ciberincidentes circunstancias tales como los ataques a sistemas de tecnologías de la información y de las comunicaciones, el fraude electrónico, el robo de identidad, o el abuso del Ciberespacio.

Artículo 15. Gestión de ciberincidentes.

1. Un ciberincidente consta de las siguientes fases, cuya gestión es responsabilidad del Equipo de Respuesta a Ciberincidentes (ERC) que se formaliza en los apartados 2 a 4 del presente artículo:
    a) Fase de preparación: el Ayuntamiento debe contemplar la creación y formación de un Equipo de Respuesta a Ciberincidentes, y la utilización de las herramientas y recursos necesarios. Para ello, atendiendo a lo dispuesto en los Anexos I y II del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, y previo el correspondiente análisis de riesgos, deben haberse identificado y desplegado un determinado conjunto de medidas de seguridad, si bien también debe tomarse en consideración el hecho de que, incluso tras la implantación de tales medidas, persistirá un riesgo residual, o apetencia del riesgo, que también debe ser gestionado.
    b) Fase de detección, análisis y notificación: el Ayuntamiento debe implantar las antedichas medidas con el objeto de detectar posibles brechas de seguridad de los sistemas de información en el conjunto del Ayuntamiento y sus entidades vinculadas o dependientes; así como para proceder a su análisis, en la fase de detección, análisis y notificación, desencadenando los procesos de notificación a los que hubiere lugar.
    c) Fase de contención, erradicación y recuperación: ante la presencia de un ciberincidente, el Equipo de Respuesta a Ciberincidentes, atendiendo a la peligrosidad del mismo, deberá intentar, en primera instancia, mitigar su impacto, procediendo después a su eliminación de los sistemas afectados y tratando finalmente de recuperar el sistema al modo de funcionamiento normal. Durante esta fase se debe persistir cíclicamente en el análisis de la amenaza, de cuyos resultados se deben desprender paulatinamente nuevos mecanismos de contención y erradicación.
    d) Fase de actividad post-ciberincidente: tras el ciberincidente, el Jefe del Equipo de Respuesta a Ciberincidentes, emitirá un informe a la Alcaldía o Concejal que tenga delegadas las competencias en Administración electrónica, sobre el Ciberincidente que detallará su causa originaria y su coste, especialmente en términos de compromiso de la información y

de impacto en los servicios prestados, y las medidas que el Ayuntamiento debe tomar para prevenir futuros ciberincidentes de naturaleza similar.

2. Para la adecuada gestión de las fases mencionadas se hará uso de la Guía CCN- STIC 403 Gestión de Incidentes de Seguridad.
3. El Ayuntamiento conformará un Equipo de Respuesta a Ciberincidentes, compuesto por técnicos en Tecnologías de la Información y de las Comunicaciones y en Administración Electrónica, así como por Letrado Consistorial, Técnico de Administración General y Técnico de Administración electrónica pertenecientes al Grupo de Proyecto para el impulso de la Administración electrónica, con las funciones que se derivan del presente Reglamento.
4. El Equipo de Respuesta a Ciberincidentes debe ser formalmente designado por resolución de Alcaldía o del Concejal competente en materia de Tecnologías de la Información y de las Comunicaciones y de Administración Electrónica.
5. El Equipo de Respuesta a Ciberincidentes estará dirigido por un Jefe de Equipo, cuyas funciones principales son la supervisión de todas las fases de gestión del ciberincidente, el informe post-ciberincidente y el aseguramiento de la comunicación continuada entre todos los miembros del Equipo, así como con terceras partes, si procede.
6. En todo caso, ante la sospecha de que un ciberincidente puede ocurrir, ha ocurrido o está ocurriendo, se informará al Sistema de Alerta Temprana de Red SARA (SAT- SARA) o al Sistema de Alerta Temprana de Internet (SAT-INET), del Centro Criptológico Nacional, según proceda.

Artículo 16. Clasificación de los ciberincidentes.

1. Los ciberincidentes se clasificarán de acuerdo con una taxonomía que tome en consideración como mínimo los siguientes factores:
   a) Tipo de amenaza: código dañino, intrusiones, fraude, etc.
   b) Origen de la amenaza: Interna o externa.
   c) Categoría de seguridad de los sistemas afectados.
   d) Perfil de los usuarios afectados, su posición en la estructura organizativa del Ayuntamiento y, en consecuencia, sus privilegios de acceso a información sensible o confidencial.
   e) Número y tipología de los sistemas afectados.
   f) Impacto que el incidente puede tener sobre el todo del Ayuntamiento y sus entidades vinculadas o dependientes, desde los puntos de vista de la protección de la información, la prestación de los servicios, la conformidad legal y la imagen pública.
   g) Requerimientos legales y reguladores.
2. El Jefe del Equipo de Respuesta a Ciberincidentes debe determinar, a partir de la combinación de uno o varios de estos factores, la

decisión de crear un ciberincidente, su peligrosidad y las prioridades de actuación.

3. Todos los ciberincidentes detectados se clasificarán de acuerdo con la siguiente taxonomía:

CLASIFICACIÓN DE LOS CIBERINCIDENTES		
Clase de Ciberincidente	**Descripción**	**Tipo de ciberincidente**
Código dañino	Software cuyo objetivo es infiltrarse o dañar un ordenador, servidor u otro dispositivo de red, sin el conocimiento de su responsable o usuario y con finalidades muy diversas.	Virus
		Gusanos
		Troyanos
		Spyware
		Rootkit
		Ransomware (secuestro informático)
		Herramienta para Acceso Remoto (Remote Access Tool o RAT)
Disponibilidad	Ataques dirigidos a poner fuera de servicio los sistemas, al objeto de causar daños en la productividad y/o la imagen de las instituciones atacadas.	Denegación [Distribuida] del Servicio DoS / DDoS
		Fallo (Hardware/Software)
		Error humano
		Sabotaje
Obtención de información	Ataques dirigidos a recabar información fundamental que permita avanzar en ataques más sofisticados, a través de ingeniería social o de identificación de vulnerabilidades.	Identificación de vulnerabilidades (scanning)
		Sniffing
		Ingeniería social
		Phishing
Intrusiones	Ataques dirigidos a la explotación de vulnerabilidades de diseño, de operación o de configuración de diferentes tecnologías, al objeto de introducirse de forma fraudulenta en los sistemas de	Compromiso de cuenta de usuario
		Defacement (desfiguración)
		Cross-Site Scripting (XSS)

	una organización.	Cross-Site Request Forgery (CSRF) Falsificación de petición entre sitios cruzados
		Inyección SQL
		Spear Phishing
		Pharming
		Ataque de fuerza bruta
		Inyección de Ficheros Remota
		Explotación de vulnerabilidad software
		Explotación de vulnerabilidad hardware
Compromiso de la información	Incidentes relacionados con el acceso y fuga (Confidencialidad), modificación o borrado (Integridad) de información no pública.	Acceso no autorizado a información
		Modificación y borrado no autorizado de información
		Publicación no autorizada de información
		Exfiltración de información
Fraude	Incidentes relacionados con acciones fraudulentas derivadas de suplantación de identidad, en todas sus variantes.	Suplantación / Spoofing
		Uso de recursos no autorizado
		Uso ilegítimo de credenciales
		Violaciones de derechos de propiedad intelectual o industrial
Contenido abusivo	Ataques dirigidos a dañar la imagen de la organización o a utilizar sus medios electrónicos para otros usos ilícitos (tales como la publicidad, la extorsión o, en general la ciberdelincuencia).	Spam (Correo Basura)
		Acoso/extorsión/ mensajes ofensivos
		Pederastia/ racismo/ apología de la violencia/delito, etc.
Política de seguridad	Incidentes relacionados por violaciones de usuarios de las políticas de seguridad aprobadas por la organización.	Abuso de privilegios por usuarios
		Acceso a servicios no autorizados
		Sistema desactualizado
		Otros
Otros	Otros incidentes no incluidos en los apartados anteriores	

Artículo 17. Detección de ciberincidentes.

1. Dada la dificultad para determinar con precisión en todos los casos si se ha producido o no un ciberincidente y, si es así, identificar su tipo y evaluar a priori su peligrosidad, el Jefe del Equipo de Respuesta a Ciberincidentes valorará dos tipos de fuentes, si se dispone de ellas: los precursores y los indicadores, entendiéndose como precursor un indicio de que puede ocurrir un incidente en el futuro; y como indicador un indicio de que un incidente puede haber ocurrido o puede estar ocurriendo ahora.
2. De igual modo, dado que la mayoría de los ataques no tienen precursores identificables o detectables, desde la perspectiva del objetivo, debe prestarse especial atención a precursores tales como las entradas en los ficheros de log de los servidores web, con los resultados de un escáner de vulnerabilidades; el anuncio de un nuevo fragmento de software o secuencia de comandos, dirigido a atacar una vulnerabilidad que podría estar presente en los sistemas del Ayuntamiento; o las amenazas explícitas procedentes de grupos o entidades concretos, anunciando ataques a organizaciones objetivo. En cualquier caso, tales fuentes no tienen carácter exhaustivo.
3. En ausencia de precursores identificables, se prestará también especial atención a la existencia de indicadores como el sensor de intrusión de una red, que emita una alerta cuando ha habido un intento de desbordamiento de búfer contra un servidor de base de datos; las alertas generadas por software antivirus; la presencia de un nombre de archivo con caracteres inusuales; un registro en los ficheros de log sobre un cambio no previsto en la configuración de un host; los ficheros de log de una aplicación; las advertencias de reiterados intentos fallidos de identificación desde un sistema externo desconocido; la detección de un número importante de correos electrónicos rebotados con contenido sospechoso; una desviación inusual del tráfico de la red interna, etc.
4. Puesto que la determinación de si un evento en particular es en realidad un ciberincidente constituye, en ocasiones, una cuestión de apreciación y juicio, debe intercambiarse la información del supuesto ciberincidente entre los diferentes miembros del Equipo de Respuesta a Ciberincidentes.

Artículo 18. Peligrosidad de los ciberincidentes.

1. Además de tipificar los ciberincidentes dentro de un determinado grupo o tipo, la gestión de los mismos exige determinar la peligrosidad potencial que el ciberincidente posee. Para ello, deben fijarse ciertos criterios de determinación de la peligrosidad con los que comparar las evidencias que se disponen del ciberincidente, en sus estadios iniciales.
2. A efectos del presente Reglamento, la peligrosidad de un ciberincidente dado se asignará a uno de una escala de cinco

valores. Esta escala, de menor a mayor peligrosidad, es la que se muestra a continuación.

Nivel	Peligrosidad
1	BAJO
2	MEDIO
3	ALTO
4	MUY ALTO
5	CRÍTICO

3. En lo que concierne al nivel de peligrosidad de los ciberincidentes, éste se determinará a partir de los criterios que se muestran en el siguiente cuadro.

CRITERIOS DE DETERMINACIÓN DEL NIVEL DE PELIGROSIDAD DE LOS CIBERINCIDENTES			
NIVEL	AMENAZA(S) SUBYACENTE(S) MÁS HABITUAL(ES)	VECTOR DE ATAQUE	CARACTERÍSTICAS POTENCIALES DEL CIBERINCIDENTE
CRÍTICO	**Ciberespionaje**	Amenazas Avanzadas Persistentes (APTs), campañas de malware, interrupción de servicios, compromiso de sistemas de control industrial, incidentes especiales, etc.	- Capacidad para exfiltrar información muy valiosa,en cantidad considerable y en poco tiempo.
MUY ALTO	**Interrupción de los Servicios de Tecnologías de la Información y las Comunicaciones / Exfiltración de datos / Compromiso de los servicios**	-Códigos dañinos confirmados de Alto Impacto (RAT, troyanos enviando datos, rootkit, etc.) - Ataques externos con éxito.	- Capacidad para exfiltrar información valiosa, en cantidad apreciable. - Capacidad para tomar el control de los sistemas sensibles, en cantidad considerable.

ALTO	**Toma de control de los sistemas / Robo y publicación o venta de información sustraída / Ciberdelito / Suplantación**	- Códigos dañinos de Medio Impacto (virus, gusanos, troyanos). - Ataques externos – compromiso de servicios no esenciales (DoS / DDoS). - Tráfico DNS con dominios relacionados con APTs o campañas de malware. - Accesos no autorizados / Suplantación / Sabotaje. - Cross-Site Scripting / Inyección SQL.	- Capacidad para exfiltrar información valiosa. - Capacidad para tomar el control de ciertos sistemas.
MEDIO	**Logro o incremento significativo de capacidades ofensivas /** **Desfiguración de páginas web / Manipulación de información**	- Descargas de archivos sospechosos. - Contactos con dominios o direcciones IP (Internet Protocol)sospechosas. - Escáneres de vulnerabilidades. Códigos dañinos de - Bajo Impacto (adware, spyware, etc.) - Sniffing / Ingeniería social.	- Capacidad para exfiltrar un volumen apreciable de información. - Capacidad para tomar el control de de algún sistema.
BAJO	**Ataques a la imagen / menosprecio / Errores y fallos**	- Políticas. - Spam sin adjuntos. - Software desactualizado. - Acoso / coacción / comentarios ofensivos. - Error humano / Fallo HW-SW.	- Escasa capacidad para exfiltrar un volumen apreciable de información. - Nula o escasa capacidad para tomar el control de sistemas.

Artículo 19. Nivel de impacto del ciberincidente.

1. El impacto de un ciberincidente en el Ayuntamiento o sus entidades vinculadas o dependientes debe determinarse evaluando las consecuencias que tal ciberincidente ha tenido en sus funciones, en sus activos o en los individuos afectados. Por tanto, el Equipo de Respuesta a Ciberincidentes priorizará la gestión de los mismos de conformidad, aunque no de manera exclusiva, con los siguientes criterios:
    a) Impacto Funcional del Ciberincidente: El Equipo de Respuesta de Ciberincidentes debe considerar la forma en que el

ciberincidente puede impactar en la funcionalidad de los sistemas afectados.

b) Impacto del ciberincidente en la información o los servicios: Puesto que los ciberincidentes pueden afectar a la confidencialidad y la integridad de la información tratada por el Ayuntamiento o sus entidades vinculadas o dependientes, o a la disponibilidad de los servicios prestados, el Equipo de Respuesta a Ciberincidentes debe considerar el modo en que el ciberincidente puede impactar en el desenvolvimiento competencial del Ayuntamiento o en su imagen pública.

c) Recuperación del ciberincidente: Puesto que el tipo de ciberincidente y la superficie de activos atacada determinará el tiempo y los recursos que deben destinarse a la recuperación, el Equipo de Respuesta a Ciberincidentes, con la ayuda oportuna de otras unidades del Ayuntamiento, si procede, debe considerar el esfuerzo necesario para regresar a la situación pre-ciberincidente y su oportunidad.

2. Estos criterios pueden cambiar si en el transcurso del proceso de su gestión se modificasen las circunstancias o conocimiento que se tiene del ciberincidente.
3. El nivel de impacto potencial de un ciberincidente se determinará de conformidad con los criterios establecidos en el siguiente cuadro:

Nivel	Descripción
I0 – IRRELEVANTE	No hay impacto apreciable sobre el sistema No hay daños reputacionales apreciables
I1 – BAJO	La categoría más alta de los sistemas de información afectados es baja El ciberincidente precisa para resolverse menos de 1 jornada/persona Daños reputacionales puntuales, sin eco mediático
I2 – MEDIO	La categoría más alta de los sistemas de información afectados es media Afecta a más de 10 equipos con información cuya máxima categoría es baja El ciberincidente precisa para resolverse entre 1 y 10 jornadas/persona Daños reputacionales apreciables, con eco mediático (amplia cobertura en los medios de comunicación)

I3 – ALTO	La categoría más alta de los sistemas de información afectados es alta Afecta a más de 50 equipos con información cuya máxima categoría es baja Afecta a más de 10 equipos con información cuya máxima categoría es media El ciberincidente precisa para resolverse entre 10 y 20 jornadas/persona Daños reputacionales de difícil reparación, con eco mediático (amplia cobertura en los medios de comunicación) y afectando a la reputación de terceros
I4 – MUY ALTO	Afecta a sistemas clasificados con nivel reservado Afecta a más de 100 equipos con información cuya máxima categoría es baja Afecta a más de 50 equipos con información cuya máxima categoría es media Afecta a más de 10 equipos con información cuya máxima categoría es alta El ciberincidente precisa para resolverse entre 20 y 50 jornadas/persona Daños reputacionales a la imagen del Gobierno local, de la Administración Municipal, o de cualquier otro Ejecutivo o Administración Afecta apreciablemente a actividades oficiales o misiones en el extranjero Afecta apreciablemente a una infraestructura crítica
I5 - CRÍTICO	Afecta a sistemas clasificados con nivel secreto Afecta a más de 100 equipos con información cuya máxima categoría es media Afecta a más de 50 equipos con información cuya máxima categoría es alta Afecta a más de 10 equipos con información clasificada con nivel reservado El ciberincidente precisa para resolverse más de 50 jornadas/persona Afecta apreciablemente a la seguridad nacional Afecta gravemente a una infraestructura crítica

Artículo 20. Documentación de los ciberincidentes.

1. El Equipo de Respuesta a Ciberincidentes debe documentar el desarrollo del ciberincidente y las acciones que se han llevado a cabo en cada momento, correspondientes a las fases de detección, contención, erradicación y recuperación.
2. El documento mencionado debe contener al menos tanto nivel de detalle como el que la Guía de Seguridad de las Tecnologías de la Información y las Comunicaciones CCN-STIC-817: Esquema Nacional de Seguridad: Gestión de Ciberincidentes prevé para el seguimiento y la tipificación de las causas de los mismos, a cuyo fin se elaborarán los oportunos modelos normalizados.
3. De igual modo, se hará uso de las métricas y los indicadores codificados en la mencionada Guía.

Artículo 21. Recolección y custodia de evidencias.

1. Aunque el motivo principal para la recolección de las evidencias de un ciberincidente es ayudar a su resolución, también puede ser necesaria para iniciar procesos de naturaleza legal. Por tanto, debe documentarse claramente cómo se han obtenido y custodiado las evidencias, siempre conforme a lo dispuesto en la legislación vigente. De resultar necesario, el Equipo de Respuesta a Ciberincidentes requerirá informe interno a la Asesoría Jurídica, el Centro de Proceso de Datos, el Grupo de Proyecto para el Impulso de la Administración Electrónica, la Policía Judicial, o cualquier otro que estime pertinente; así como a terceras partes externas especializadas, como otras Fuerzas y Cuerpos de Seguridad o la Fiscalía para la Criminalidad Informática.
2. Debe mantenerse un registro detallado de todas las evidencias, que incluya como mínimo:
    a) La identificación de la información, por ejemplo, la localización, el número de serie, número de modelo, el nombre de host, dirección MAC (Media Access Control) y direcciones IP (Internet Protocol) de los ordenadores afectados.
    b) Nombre, cargo y teléfono de cada persona que ha recogido o gestionado evidencias durante la investigación del ciberincidente.
    c) Fecha y hora de cada ocasión en la que ha sido tratada cada evidencia.
    d) Ubicaciones donde se custodiaron las evidencias.
3. Debe comenzarse el acopio de evidencias tan pronto como se detecte un ciberincidente, obteniendo inmediatamente, siempre que sea posible, una instantánea del sistema atacado, dejándolo inaccesible y garantizando su integridad, antes de tratar las copias que se realicen del sistema atacado con diferentes tipos de herramientas que, de otro modo, podrían alterar parte de la información o el estado de los sistemas comprometidos.
4. De manera reglamentaria, el Ayuntamiento redactará y aprobará las normas que deben regir la custodia y la conservación de evidencias digitales, que como mínimo habrán de satisfacer los mismos requisitos que se determinen para elarchivo electrónico único, así como definir los mecanismos de custodia de los componentes físicos de las evidencias, como discos duros, otras herramientas de almacenamiento, dispositivos móviles o sistemas que hayan sido puestos en compromiso.

Artículo 22. Intercambio de información y comunicación de ciberincidentes.

1. Además de la preceptiva notificación de los ciberincidentes al CCN-CERT, el Ayuntamiento se comunicará siempre que sea necesario con terceros, y específicamente con Fuerzas y Cuerpos de Seguridad y

medios de comunicación social. El resto de las comunicaciones con otros actores se llevarán a cabo a través del CCN-CERT, en su función de Nodo de Intercambio de Información de Ciberincidentes en los Sistemas de Información de las Administraciones Públicas.

2. Independientemente de lo anterior, el Equipo de Respuesta a Ciberincidentes debe analizar con las unidades pertinentes del Ayuntamiento o sus entidades vinculadas o dependientes, y particularmente con la Asesoría Jurídica, el Grupo de Proyecto para el impulso de la administración electrónica, el Centro de Proceso de Datos y con la unidad con competencias en relaciones institucionales, los criterios y procedimientos de información a terceros ante la ocurrencia de un ciberincidente. De lo contrario, podría darse el caso de que información confidencial contenida en la información de los ciberincidentes pueda entregarse a terceros no autorizados, lo cual, además de representar un daño a la imagen del Ayuntamiento y una falta grave de incumplimiento legal, podría dar lugar a la exigencia de responsabilidad patrimonial de la entidad, por daños y perjuicios ocasionados a terceros.
3. La coordinación y el intercambio de información con los organismos adecuados debe contribuir al fin de fortalecer la capacidad del Ayuntamiento, así como de otras administraciones, para responder con eficacia a los ciberincidentes.
4. En la medida en que la capacidad de responder a ciertos ciberincidentes puede que requiera el uso de herramientas que no estén disponibles para el Ayuntamiento, éste debe aprovechar su red de intercambio de información de confianza para externalizar de manera eficaz el análisis del ciberincidente a los recursos de terceros que sí tienen las capacidades técnicas adecuadas para gestionar adecuadamente el ciberincidente.

DISPOSICIONES ADICIONALES

Primera. Concurrencia con el Título VIII del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal

1. El alcance establecido para la auditoría en el artículo 34 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, no tiene como objeto auditar o verificar el cumplimiento de las medidas de seguridad establecidas por el artículo 96 del Título VIII del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. Si el sistema de información auditado según el Real Decreto 3/2010 tratase datos de carácter personal, el equipo

auditor podrá solicitar una copia de la auditoría preceptiva según el Real Decreto 1720/2007.

2. No obstante, si durante la realización de la auditoría a la que es aplicable el presente Reglamento se identificase algún incumplimiento manifiesto del Real Decreto 1720/2007, es obligación del equipo auditor comunicarlo, e incluirlo en el informe de auditoría.
3. Asimismo, es posible que se establezca previamente la realización conjunta de ambas auditorías. En esta circunstancia, que ambas auditorías coincidan en el tiempo y sean realizadas por el mismo equipo de auditoría, es necesario tener en cuenta, los aspectos comunes y diferenciados:
    a) El Título VIII del Real Decreto 1720/2007 (medidas de seguridad en el tratamiento de datos de carácter personal) se aplica tanto a ficheros automatizados como no automatizados, y muchos de sus artículos son comunes a ambos tratamientos.
    b) Los criterios para la categorización de los sistemas y el establecimiento de los niveles de seguridad en el Real Decreto 3/2010 (grado de perjuicio o impacto en el sistema o en las personas), son diferentes de los criterios seguidos en el Real Decreto 1720/2007 (tipología de datos tratados, almacenados o a los que se tiene acceso, y con algunas excepciones según la finalidad de su tratamiento) para la determinacióndel nivel de medidas de seguridad aplicables. Por tanto el auditor deberá tener en cuenta unos y otros, en sus respectivos ámbitos de aplicación.
    c) Como buenas prácticas de seguridad, el Real Decreto 3/2010 y el Real Decreto 1720/2007 coinciden en que debe existir una Política de Seguridad y un Documento de seguridad, aprobados por el Ayuntamiento y comunicados a todo el personal afectado. En el espíritu del Real Decreto 1720/2007 subyace la condición de que las medidas exigidas para los ficheros son requisitos mínimos sin perjuicio de los requisitos de otras legislaciones o que se considere necesario para la protección de los datos.
    d) La actividad también puede ser determinante, en algunos casos, en la aplicación de las medidas de seguridad. Así, el artículo 81 del Real Decreto 1720/2007 indica que a los ficheros de los que sean responsables los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones electrónicas respecto a los datos de tráfico y a los datos de localización, se aplicarán, además de las medidas de seguridad de nivel básico y medio, la medida de seguridad de nivel alto contenida en el artículo 103.

e) El Real Decreto 1720/2007 requiere determinadas medidas de seguridad, según el nivel aplicable, que pueden no derivarse necesariamente del preceptivo análisis de riesgos realizado según el Real Decreto 3/2010, y que por lo tanto, podrían no estar previstas como medidas a implantar siguiendo los requisitos de este último. A continuación se mencionan algunas de las medidas que deben estar en esta situación:
    i. Para los ficheros de cualquier nivel, se debe verificar semestralmente la fiabilidad de las copias de respaldo, de conformidad con el artículo 94.
    ii. La recuperación de datos se considera una incidencia de seguridad, de conformidad con el artículo 100 y para los niveles medio y alto, requiriendo asimismo el registro de determinada información.
    iii. El registro de accesos, de conformidad con el artículo 103 y para el nivel alto no puede ser desactivado ni deberá haber posibilidad de que sea manipulable, y se requiere una revisión mensual por el Responsable de Seguridad, que elaborará un informe sobre la revisión, y se mantendrá por dos años.
    iv. Si bien el cifrado en comunicaciones sólo se exige categóricamente para los ficheros que requieren medidas de nivel alto, su transmisión electrónica debe evitar su divulgación también para el nivel medio.
    v. En relación al control de accesos, el Real Decreto 1720/2007, de conformidad con su artículo 91 requiere la definición de perfiles de acceso.
    vi. La auditoría requerida por el artículo 96 del Real Decreto 1720/2007 también implica la revisión de los contratos de proveedores externos referidos en el Documento de Seguridad, en cuanto a determinados contenidos, según las circunstancias de la prestación del servicio.

4. Se podrán emitir dos informes diferenciados, cada uno con su objetivo y alcance, o bien indicar qué deficiencias afectan al cumplimiento de una u otra norma.
5. Consecuentemente, dado que estas dos normas son concurrentes en una gran mayoría de las medidas de seguridad a adoptar, pero diferentes en otras, el equipo auditor debe, si se realizan auditorías conjuntas, considerar y diferenciar en su planificación de la evaluación de las medidas de seguridad aplicables según la tipología de datos tratados y la finalidad de su tratamiento, por el sistema de información auditado, y determinar cuándo una revisión o prueba es válida para ambas auditorías.

Segunda. Formación.

El Ayuntamiento planificará y emprenderá las oportunas acciones formativas para que todos sus empleados, a los niveles pertinentes, estén informados, cumplan y hagan cumplir el presente Reglamento.

Tercera. Glosario.

Los términos utilizados en el presente Reglamento se incorporarán al Glosario de Administración Electrónica previsto en la "Ordenanza Municipal de Administración Electrónica del Excmo. Ayuntamiento de Cartagena".

DISPOSICION FINAL

Primera. Entrada en vigor.

El presente Reglamento será objeto de aprobación y publicación de acuerdo con los trámites legales oportunos, se publicará en la sede electrónica del Ayuntamiento y en su portal de transparencia y entrará en vigor en el plazo establecido en el artículo 70.2 y 65 de la Ley 7/1985, de 2 de abril, reguladora de las Bases del Régimen Local, a partir de su publicación en el Boletín Oficial.

ANEXO I: MODELO DE ACUERDO DE CONFIDENCIALIDAD (normativo)

Los contenidos de los modelos de confidencialidad que se incluyen en este Anexo, tendrán la consideración de requisitos mínimos. Las responsabilidades de su aplicación, en relación a sus respectivos equipos involucrados, en cualquier medida, en la auditoría, corresponden tanto al Ayuntamiento como a los equipos de auditoría y a los responsables de los sistemas de información auditados.

Datos de carácter personal

Las tareas de auditoría a realizar no conllevan necesariamente el tratamiento posterior ni simultáneo de datos de carácter personal. Pero, por la naturaleza de los servicios, es posible que se tenga acceso a los mismos. Estos servicios no se encuadran exactamente en la figura de "encargado del tratamiento" establecida en el artículo 3 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Sin embargo, sí podría considerarse aplicable el artículo 83 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

Dado que, en alguna circunstancia, se podría acceder a este tipo de datos, el equipo de auditoría XXXX se compromete, en cumplimiento de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, a tratar los datos conforme a las instrucciones del responsable de los datos de carácter personal (Responsable de Fichero) a los que pudiera

acceder, que no los aplicará o utilizará con fin distinto al que figure en este acuerdo o contrato, ni los comunicará, ni siquiera para su conservación, a otras personas.

XXXX declara conocer la legislación vigente en materia de protección de datos, y el equipo de auditoría está instruido en estos requisitos. Por lo tanto, en caso de tener lugar este acceso, como consecuencia de los servicios a prestar, se compromete a observar los requisitos establecidos en esta legislación.

De igual forma el Ayuntamiento, al cual pertenece el sistema auditado se compromete a no difundir ni utilizar para otros fines que los de la realización de la auditoría, cualquier dato de carácter personal del equipo de auditoría.

Información del sistema de información auditado.

XXXX se compromete a no difundir información alguna (procesos, sistemas, medidas de seguridad, y cualquier otra información relacionada o no con el sistema de información auditado, incluyendo el informe de auditoría) que se pueda conocer o a la que se tenga acceso durante la realización de la auditoría. En este sentido están instruidos todos los integrantes del equipo de auditoría, que han firmado sus respectivos acuerdos de confidencialidad.

Una copia de los documentos de trabajo que se elaboren para la realización de la presente auditoría será custodiada por XXXX, como evidencia del trabajo realizado.

Firmantes del acuerdo de confidencialidad.

Los firmantes del acuerdo de confidencialidad serán todos y cada uno de los miembros del equipo auditor, incluyendo a expertos, con independencia del momento en el que se incorporen al mismo.

E-EMGDE: ESQUEMA DE METADATOS PARA LA GESTIÓN DE DOCUMENTOS ELECTRÓNICOS (informativo)

El Esquema de Metadatos para la Gestión de Documentos Electrónicos (Documentación complementaria a la Norma Técnica de Interoperabilidad de Política de Gestión de documentos electrónicos), tiene carácter meramente informativo y debe servir para la elaboración del perfil de aplicación, de obligado cumplimiento, previsto en el artículo 5.2 del presente Reglamento.

REFERENCIAS

Guía de seguridad CCN-STIC-802: Esquema Nacional de Seguridad: Guía de Auditoría: Guía de Seguridad de las Tecnologías de la Información y las Comunicaciones. Centro Criptológico Nacional, 2010

Guía de seguridad de las Tecnologías de la Información y las Comunicaciones CCN- STIC-817: Esquema Nacional de Seguridad: Gestión de Ciberincidentes ISO/IEC 27037: Information technology: Security

techniques: Guidelines for identification, collection, acquisition, and preservation of digital evidence. International Organization for Standardization, 2012

La Junta de Gobierno Local acuerda aprobar, por unanimidad, al anterior propuesta.

6. PROYECTO DE REGLAMENTO DE PROTECCIÓN DE DATOS DEL EXCMO. AYUNTAMIENTO DE CARTAGENA.

Con fecha de 22 de diciembre de 2016, se ha emitido informe por la Jefe de Servicios Administrativos Generales del siguiente contenido literal:

"La Ley 39/2015 de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas impone la obligación y el derecho de los ciudadanos a relacionarse electrónicamente con las Administraciones Públicas, de tal manera que éstas están obligadas a disponer de las herramientas y recursos necesarios para garantizar esta relación electrónica con los obligados por la Ley y con las personas físicas que así lo prefieran; a tramitar electrónicamente los expedientes de forma que se disponga de un registro electrónico general, interoperable con el resto de registros electrónicos de las administraciones; determinar el sistema de identificación y firma electrónica para el acceso electrónico a los trámites o procedimientos administrativos; disponer de un sistema de información que soporte el Registro Electrónico de Apoderamientos, en el que conste el bastanteo de poder; identificar los funcionarios habilitados en las oficinas de asistencia en materia de registro para la asistencia en lo referente a la identificación y firma electrónica, presentación de solicitudes y obtención de copias auténticas; disponer de una carpeta ciudadana para consultar el estado de tramitación de los expedientes y obtener copia de los documentos; disponer igualmente de un sistema de notificación electrónica; archivar electrónicamente; garantizar el derecho a la información y transparencia; etc.

Así mismo, el artículo 3.2 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, establece que las administraciones públicas se relacionarán entre sí y con sus órganos, organismos públicos y entidades vinculadas o dependientes a través de medios electrónicos.

Como resultado de lo expuesto, en la actuación administrativa electrónica se accede y manejan un sin fin de datos, cuya protección les es exigible a las Administraciones Públicas por la LO 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y por el RD 1720/2007, de 21 de diciembre, por el que se aprueba su reglamento de

desarrollo. No obstante, al citado cuerpo normativo, hay que sumar un conjunto de normas de carácter técnico y jurídico que inciden directamente en la necesidad de que el Ayuntamiento de Cartagena, se dote de una norma reguladora que incida en el cumplimiento de las obligaciones que las normas técnicas y jurídicas imponen, para establecer unas conductas organizativas donde la protección de datos sea un eje transversal que ligue toda su actuación administrativa, a fin de garantizar y proteger las libertades públicas y los derechos fundamentales de los ciudadanos y especialmente su derecho al honor y a la intimidad personal y familiar, y que sirva como base para los empleados públicos municipales acerca de la manera de actuar en su relación con los ciudadanos en todo lo referente al tratamiento de datos personales.

El 4 de mayo de 2016, se publicó en el Diario Oficial de la Unión Europea el Reglamento (UE) 2016/679, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta a la protección de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos) con efecto del 25 de mayo de 2018.

El Real Decreto 3/2010, de 1 de octubre, por el que se aprueba el Esquema Nacional de Seguridad, fue sometido previo a su aprobación, a informe de la Agencia Española de Protección de Datos. En su Exposición de Motivos se contiene que: "En este Real Decreto se concibe la seguridad como una actividad integral, en la que no caben actuaciones puntuales o tratamientos coyunturales, debido a que la debilidad de un sistema la determina su punto más frágil y, a menudo, este punto es la coordinación entre medidas individualmente adecuadas pero deficientemente ensambladas. La información tratada en los sistemas electrónicos a los que se refiere este Real Decreto estará protegida teniendo en cuenta los criterios establecidos en la Ley Orgánica 15/1999, de 13 de diciembre". Así mismo, a lo largo de su contenido y en las Normas Técnicas que desarrollan el ENS, se hace innumerables referencias a la protección de datos en el tratamiento electrónico. Según su artículo 27.2 y 3: "2. Cuando un sistema al que afecte el presente Real Decreto maneje datos de carácter personal le será de aplicación lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y normativa de desarrollo, sin perjuicio de los requisitos establecidos en el Esquema Nacional de Seguridad. 3. Las medidas a las que se refieren los apartados 1 y 2 tendrán la condición de mínimos exigibles, y podrán ser ampliados por causa de la concurrencia indicada o del prudente arbitrio del responsable de la seguridad del sistema, habida cuenta del estado de la tecnología, la naturaleza de los servicios prestados y la información manejada, y los riesgos a que están expuestos.

Por su parte, el Real Decreto 4/2010, de 1 de octubre, por el que se aprueba el Esquema Nacional de Interoperabilidad, informado con

carácter previo también a su aprobación por la AEPD, establece en su artículo 8.1 lo siguiente: "1. Las Administraciones públicas establecerán y publicarán las condiciones de acceso y utilización de los servicios, datos y documentos en formato electrónico que pongan a disposición del resto de Administraciones especificando las finalidades, las modalidades de consumo, consulta o interacción, los requisitos que deben satisfacer los posibles usuarios de los mismos, los perfiles de los participantes implicados en la utilización de los servicios, los protocolos y criterios funcionales o técnicos necesarios para acceder a dichos servicios, los necesarios mecanismos de gobierno de los sistemas interoperables, así como las condiciones de seguridad aplicables. Estas condiciones deberán en todo caso resultar conformes a los principios, derechos y obligaciones contenidos en la Ley Orgánica 15/1999, de 13 de diciembre (RCL 1999, 3058) , de Protección de Datos de Carácter Personal y su normativa de desarrollo, así como a lo dispuesto en el Esquema Nacional de Seguridad, y los instrumentos jurídicos que deberán suscribir las Administraciones públicas requeridoras de dichos servicios, datos y documentos". Este principio que patente en las Normas Técnicas de Interoperabilidad aprobadas en virtud de lo ordenado en el ENI tales como , la NTI de Política de Gestión de Documentos Electrónicos; NTI de Protocolos de Intermediación de Datos; NTI de Documento Electrónico; NTI de de expediente electrónico, etc.

A la vista lo expuesto, se considera adecuado la regulación interna del tratamiento de datos como base para crear una cultura adecuada y una obligada conducta de los empleados públicos en cuanto al manejo de los mismos, dentro del marco de la legalidad existente."

Consta en el expediente informe Técnico de fecha 22 de diciembre de 2016,

En virtud de todo lo anteriormente expuesto, en el ejercicio de las competencias que tengo atribuidas, elevo a la Junta de Gobierno Local la siguiente PROPUESTA para que, previa deliberación adopte, si lo considera procedente, el siguiente **ACUERDO:**

UNICO: La aprobación del Proyecto de Reglamento de Protección de Datos del Excmo. Ayuntamiento de Cartagena que se acompaña a continuación.

No obstante, la Junta de Gobierno Local resolverá lo que mejor proceda.= Cartagena, a 23 de diciembre de 2016.= EL CONCEJAL DELEGADO DEL ÁREA DE HACIENDA E INTERIOR.= Firmado, Francisco Aznar García, rubricado.

El referido Proyecto de Reglamento es del siguiente tenor literal:

REGLAMENTO DE PROTECCIÓN DE DATOS DEL EXCELENTÍSIMO AYUNTAMIENTO DE CARTAGENA

EXPOSICIÓN DE MOTIVOS

Las administraciones, en sus relaciones con la ciudadanía, recopilan gran cantidad de datos personales, necesarios para la adecuada gestión de sus procedimientos y la prestación de un mejor servicio, pero cuya protección resulta obligada en defensa de la privacidad de las personas. Sin embargo, la protección de datos es un derecho muy poco conocido por parte de la propia ciudadanía, a pesar del ingente volumen de memorias, informes preceptivos, sentencias y resoluciones, que desde la Agencia Española de Protección de Datos y el Poder Judicial se han venido emitiendo en los últimos años. Tampoco todas las administraciones son conscientes de que es preciso definir una conducta organizativa donde la protección de datos sea un eje transversal que ligue toda su actuación. Se hace por tanto necesario un análisis de las obligaciones de las mismas en materia de protección de datos y un estudio de la casuística más frecuente y de las colisiones que la aplicación de este derecho puede tener con otros y, con todo ello, establecer un marco normativo, como el que viene dado por el presente Reglamento.

Para la redacción del mismo se han tenido en cuenta las previsiones contenidas en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, posteriormente complementada por el 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. También se ha tomado en consideración, en lo que procede, el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), a entrar en vigor el 25 de mayo de 2018. De igual modo, se han explorado los Códigos Tipo de carácter voluntario inscritos en la Agencia Española de Protección de Datos, habiéndose optado, en lo que concierne al presente Reglamento, por realizar una adaptación del Código Tipo para las entidades locales adheridas a EUDEL (Asociación de Municipios Vascos-Euskadiko Udalen Elkartea), en la medida en que es en absoluto similar al funcionamiento del Ayuntamiento de Cartagena y sus entidades vinculadas o dependientes.

Resultado del mencionado análisis es el presente Reglamento, que se estructura en cuatro capítulos, dos disposiciones adicionales, una disposición transitoria y dos disposiciones finales. El primer Capítulo – Disposiciones generales – determina el objeto y el alcance del presente Reglamento, así como su ámbito de aplicación y el concepto de datos de carácter personal.

El segundo Capítulo – Derechos de los ciudadanos – codifica aquellos derechos que vienen recogidos por Ley y especifica el modo en que deben ser ejercitados en el marco del Ayuntamiento y sus entidades vinculadas o

dependientes: acceso, rectificación, cancelación, oposición, impugnación, indemnización y tutela.

De particular importancia resulta el Capítulo III – Obligaciones de la Administración y su personal -, en el que se detallan aquellos aspectos que el Ayuntamiento, sus entidades vinculadas o dependientes y los empleados a su cargo, están obligados a cumplir con respecto a la protección de datos de carácter personal, ya sea en soporte físico o electrónico. Especial mención se hace a la obligatoriedad de disponer de un Documento de Seguridad, en los términos previstos en el artículo 88 del mencionado Real Decreto 1720/2007.

El cuarto Capítulo - Concurrencia del derecho a la protección de datos de carácter personal con otros derechos – contribuye a resolver aquellas cuestiones que puedan plantearse en lo que se refiere a una potencial colisión entre el derecho a la protección de datos de carácter personal y otros derechos de la ciudadanía.

La Disposición Adicional primera prevé un plan anual de formación en la materia para todos los empleados municipales, así como la publicación de un decálogo de protección de datos de carácter personal. La Disposición Adicional Segunda prevé la incorporación de los términos utilizados en el presente Reglamento al Glosario codificado en la "Ordenanza Municipal de Administración Electrónica del Excelentísimo Ayuntamiento de Cartagena".

La Disposición Transitoria Única regula la necesidad de disponer de modelos y formularios normalizados, tanto para el ciudadano, en defensa de sus intereses, como para el Ayuntamiento y sus entidades vinculadas o dependientes, en su funcionamiento cotidiano.

La Disposición Final Primera establece el régimen de modificación y actualización del presente Reglamento, con especial atención a la progresiva adecuación del funcionamiento del Ayuntamiento y sus entidades vinculadas o dependientes al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), siendo el plazo máximo para tal adecuación el 25 de mayo de 2018. Por último, la Disposición Final Segunda fija el plazo de su entrada en vigor.

CAPÍTULO I
Disposiciones generales

Artículo 1. Objeto.

El presente Reglamento tiene por objeto regular el tratamiento de los datos de carácter personal que realiza el Ayuntamiento de Cartagena y sus entidades vinculadas o dependientes, así como las sociedades dependientes o vinculadas a éste cuando su capital sea de mayoría pública y ejerzan potestades públicas, a fin de garantizar y proteger las libertades públicas y los derechos fundamentales de los ciudadanos que se relacionan con él y,

especialmente, su derecho al honor y a la intimidad personal y familiar, en el marco del respeto a lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su normativa de desarrollo.

Artículo 2. Ámbito de aplicación.

El presente Reglamento será de aplicación a todo tratamiento de los datos de carácter personal que figuren en ficheros, automatizados o no, del Ayuntamiento y sus entidades vinculadas o dependientes y a toda modalidad de uso posterior de estos datos.

Artículo 3. Datos de carácter personal.

1. Para el desempeño de las competencias que tiene atribuidas, el Ayuntamiento y sus entidades vinculadas o dependientes deben cumplir la normativa de protección de datos de carácter personal al solicitar, recoger, tratar, utilizar o ceder datos de las personas con las que se relaciona. Además, dado que se trata de un derecho fundamental de nueva generación, habrá de poner los medios necesarios para extender la nueva cultura de la protección de datos en sus procedimientos y entre el personal a su servicio.
2. El Ayuntamiento y sus entidades vinculadas o dependientes han de declarar los ficheros en la Agencia Española de Protección de Datos, antes de recabar datos de carácter personal con destino a los mismos, y ha de prestar especial atención al consentimiento de las personas cuando los datos recabados tengan la consideración de especialmente protegidos.

CAPÍTULO II
Derechos de los ciudadanos

Artículo 4. Derecho a la información sobre el uso y finalidad de los ficheros.

1. Las personas a las que desde el Ayuntamiento y sus entidades vinculadas o dependientes se soliciten datos personales deberán ser previamente informadas de modo expreso, preciso e inequívoco:

a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.
b) Del carácter obligatorio o facultativo de su respuesta a las preguntas o soluciones de información que les sean planteadas.
c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.
d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.
e) De la identidad y dirección de la persona responsable del tratamiento.

2. No será necesaria la información de los apartados b), c) y d) anteriores si se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban. No obstante, se informará siempre a las personas interesadas de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición y del órgano ante el que se podrán ejercitar tales derechos.
3. La información se proporcionará a través de un medio coherente con el sistema de recogida de los datos; las informaciones y advertencias anteriores deberán figurar claramente en los documentos, formularios, cuestionarios y otros medios, debiéndose procurar que el tipo y tamaño de la letra empleada sea el mismo que el de los demás contenidos de tales medios.
4. Si las consideraciones de diseño o composición del documento a emplear aconsejasen el recurso a un tipo o tamaño de letra más reducido, se complementará la información a suministrar a través de carteles instalados en un lugar visible y destacado en las oficinas de atención ciudadana, así como de información manifiestamente visible en los portales de internet, en la sede electrónica, en el portal de transparencia, y por cualquier otro medio, de tal modo que pueda ejercitarse el derecho objeto del presente artículo de manera inequívoca.
5. Cuando los datos de carácter personal no hayan sido recabados de la persona interesada, ésta deberá ser informada de forma expresa, precisa e inequívoca, por el Ayuntamiento y sus entidades vinculadas o dependientes tan pronto como ésta tenga conocimiento del registro de los datos, salvo que ya hubiera sido informada con anterioridad, del contenido del tratamiento, de la procedencia de los datos, de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición, y de la identidad y dirección de persona responsable del tratamiento.
6. Con el fin de llevar el derecho de información a su máxima expresión, el Ayuntamiento y sus entidades vinculadas o dependientes informarán de la existencia del presente Reglamento cuando recoja datos personales a través de formularios, indicando su ubicación en la sede electrónica, en el portal de internet del Ayuntamiento y en el portal de transparencia, para su consulta.

Artículo 5. Derecho de acceso.

1. Los ciudadanos tienen derecho a solicitar y obtener del Ayuntamiento y sus entidades vinculadas o dependientes información de sus datos de carácter personal sometidos a tratamiento, del origen de dichos datos, así como de las comunicaciones realizadas o que se prevé hacer de los mismos.
2. El derecho de acceso a que se refiere este artículo sólo podrá ser ejercitado en intervalos iguales o superiores a doce meses, salvo que

la persona interesada acredite un interés legítimo al efecto, en cuyo caso podrá ejercitarlo en cualquier momento.

Artículo 6. Derecho de rectificación.

1. Cuando la persona titular de los datos tuviera constancia de que sus datos personales tratados en un fichero son inexactos, inadecuados, incompletos o excesivos, podrá solicitar y obtener del Ayuntamiento y sus entidades vinculadas o dependientes que los rectifique, corrija o complete.

Artículo 7. Derecho de cancelación.

1. La persona titular de los datos podrá solicitar y obtener del Ayuntamiento y sus entidades vinculadas o dependientes la cancelación de los mismos cuando:

a) Hayan dejado de ser necesarios o pertinentes para la finalidad para la cual fueron recabados.
b) Se haya superado el periodo necesario para el cumplimiento de los fines para los que fueron recabados.

2. No obstante, los datos de carácter personal deberán ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre el Ayuntamiento y sus entidades vinculadas o dependientes y la persona interesada.

Artículo 8. Derecho de oposición.

1. Los ciudadanos tienen derecho a oponerse a un tratamiento de datos por el Ayuntamiento y sus entidades vinculadas o dependientes cuando, sin ser preceptivo el consentimiento previo, existan motivos fundados y legítimos relativos a su concreta situación personal.
2. Las personas interesadas pueden oponerse a un tratamiento de sus datos personales, en cualquier momento, incluso cuando siendo preceptivo el consentimiento previo, lo hubieran prestado con anterioridad.

Artículo 9. Ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

1. Cualquier petición de acceso, rectificación, cancelación u oposición sobre datos de carácter personal se realizará mediante escrito, físico, únicamente en los supuestos de personas físicas no obligadas de conformidad con el artículo 14.1 de la Ley 39/2015, de 1 de octubre, o electrónico, dirigido a la persona Responsable del Fichero del Ayuntamiento, a través del Registro General o por cualquiera de los medios previstos en la Ley 39/2015, de 1 de octubre de 2015, del Procedimiento Administrativo Común de las Administraciones Públicas. Cuando la presentación de la petición no se haga de manera presencial la acreditación de la identidad de la persona interesada se realizará de conformidad con lo dispuesto en la

Ordenanza de Administración Electrónica del Ayuntamiento de Cartagena.

2. Los derechos de acceso, rectificación, cancelación u oposición de datos son personalísimos y serán ejercidos únicamente por la persona interesada. No obstante, ésta podrá actuar a través de la persona que designe como representante legal cuando se encuentre en situación de incapacidad legal o en minoría de edad que le imposibilite el ejercicio personal de los mismos, en cuyo caso será necesario que la persona que actúe como representante legal acredite tal condición.
3. No se exigirá contraprestación alguna por el ejercicio de los derechos de acceso, rectificación, cancelación u oposición de datos de carácter personal.

Artículo 10. Derecho a la impugnación de valoraciones.

Las personas interesadas tendrán derecho a impugnar decisiones que les afecten significativamente y que se basen en valoraciones realizadas por el Ayuntamiento o sus entidades vinculadas o dependientes basadas únicamente en un tratamiento de datos destinados a evaluar determinados aspectos de su personalidad. Esta impugnación se ejercitará como derecho de oposición.

Artículo 11. Derecho a indemnización por daño o lesión en los bienes y derechos de las personas.

Las personas que, como consecuencia del incumplimiento de lo dispuesto en la normativa de protección de datos por la persona responsable o la encargada del tratamiento, sufran daño o lesión en sus bienes o derechos tendrán derecho a ser indemnizadas. Esta responsabilidad se exigirá de conformidad con lo dispuesto en la legislación reguladora del régimen de responsabilidad de las administraciones públicas.

Artículo 12. Solicitud de tutela ante la Agencia Española de Protección de Datos.

Cualquier persona interesada a la que se deniegue, total o parcialmente, el ejercicio de los derechos de acceso, rectificación, oposición o cancelación, o entienda que no se le ha facilitado o atendido el ejercicio de su derecho, podrá reclamar ante la Agencia Española de Protección de Datos para que inicie un procedimiento de tutela de sus derechos.

CAPÍTULO III
Obligaciones de la Administración y su personal

Artículo 13. Creación, modificación y supresión de ficheros.

1. La creación, modificación o supresión de ficheros corresponde al órgano competente del Ayuntamiento o a sus entidades vinculadas o dependientes. La resolución o el acuerdo por el que se aprueben los

ficheros será objeto de publicación en el Boletín Oficial de la Región de Murcia.

2. Las disposiciones de creación o de modificación de ficheros deberán indicar:

a) La identificación y la finalidad del fichero y los usos previstos para el mismo.
b) Las personas o colectivos sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos.
c) El procedimiento de recogida de los datos de carácter personal.
d) La estructura básica del fichero.
e) La descripción de los tipos de datos de carácter personal incluidos en el mismo.
f) Las cesiones de datos de carácter personal.
g) Las transferencias de datos que se prevean a países terceros, en su caso.
h) El órgano del Ayuntamiento Responsable del Fichero.
i) El servicio, sección, unidad, órgano o cargo donde se puede ejercitar los derechos de acceso, rectificación, cancelación y oposición.
j) Las medidas de seguridad, con indicación del nivel básico, medio o alto exigible.

3. Cuando el Ayuntamiento o sus entidades vinculadas o dependientes tengan dudas importantes respecto a la necesidad de crear un fichero y a la forma de realizarlo, podrán solicitar, con carácter previo a la aprobación de la disposición de carácter general, la emisión de un informe por parte de la Agencia Española de Protección de Datos. A la solicitud acompañará el proyecto de norma que quiere aprobar, en su caso, y una memoria con las dudas cuya aclaración solicita.

Artículo 14. Declaración e inscripción de ficheros.

Una vez publicada la disposición de creación del fichero en el Boletín Oficial de la Región de Murcia, se notificará a la Agencia Española de Protección de Datos para su inscripción en el Registro de Protección de Datos.

Artículo 15. Propiedad de los datos.

1. El Ayuntamiento y sus entidades vinculadas o dependientes tendrán presente, en todo momento, que los datos personales son propiedad de las personas a las que se refieren y que sólo ellas pueden decidir sobre los mismos. El Ayuntamiento y sus entidades vinculadas o dependientes harán uso de ellos sólo para aquellas finalidades para las que esté facultada debidamente y respetando en todo caso la normativa sobre protección de datos de carácter personal.
2. Los datos de carácter personal deberán ser recogidos de forma leal y lícita, por lo que se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos.

3. Los datos de carácter personal sólo podrán ser recogidos para el cumplimiento de finalidades determinadas, explícitas y legítimas.

Artículo 16. Calidad en la recogida y el tratamiento de los datos personales.

1. Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.
2. Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos, siempre que dicho tratamiento tenga carácter meramente cuantitativo.

Artículo 17. Mantenimiento y actualización adecuada de los datos personales.

1. Los datos de carácter personal serán exactos y puestos al día, de forma que respondan con veracidad a la situación actual de la persona afectada. Si los datos de carácter personal registrados resultaran ser inexactos, en todo o en parte, inadecuados, incompletos o excesivos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados, sin perjuicio de las facultades que a las personas afectadas reconocen el artículo 8 y siguientes de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
2. Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados o se haya superado el periodo necesario para el cumplimiento de los fines para los que fueron recabados.

Artículo 18. Consentimiento de la persona.

1. El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco de la persona afectada, salvo que la ley disponga otra cosa.
2. El consentimiento podrá ser revocado cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos. La revocación del consentimiento deberá realizarse necesariamente mediante escrito, físico, únicamente en los supuestos de personas físicas no obligadas de conformidad con el artículo 14.1 de la Ley 39/2015, de 1 de octubre, o electrónico, dirigido a la persona Responsable del Fichero, manifestando tal decisión y ésta deberá responder en el plazo de diez días naturales, contados a partir del día siguiente al de la recepción de la solicitud de revocación del consentimiento,

materializando, en su caso, tal revocación dentro del mismo plazo. Si los datos para cuyo tratamiento se revoca el consentimiento hubieran sido comunicados previamente, el Ayuntamiento y sus entidades vinculadas o dependientes deberán notificar la revocación del consentimiento efectuada a quien se hayan comunicado, en el caso de que se mantenga el tratamiento por este último.

Artículo 19. Recogida de datos especialmente protegidos.

1. Respecto a los datos personales relativos a la salud, éstos sólo podrán ser recabados y tratados cuando por razones de interés general así lo disponga una ley o cuando la persona interesada consienta expresamente. El personal al servicio del Ayuntamiento y de sus entidades vinculadas o dependientes directamente relacionado con la salud de los trabajadores podrá tratar los datos de carácter personal relativos a la salud de las personas que atiendan, de acuerdo con lo dispuesto en la normativa vigente en materia de sanidad y de protección de la salud y prevención de riesgos laborales.
2. El tratamiento de datos relativos a ideología, religión, creencias y afiliación sindical, requiere el consentimiento expreso y por escrito de la persona interesada. Los datos de carácter personal que se refieran a la vida sexual, salud u origen racial de las personas sólo serán recabados, tratados y cedidos cuando por razones de interés público así lo establezca una ley o la persona interesada consienta expresamente. En el caso en que se recaben datos relativos a la ideología, la religión o las creencias de la persona interesada, ésta será advertida de su derecho a no consentir el tratamiento de tales datos.

Artículo 20. Facilitación a las personas del ejercicio de sus derechos.

1. El Ayuntamiento y sus entidades vinculadas o dependientes no sólo permitirán, sino que facilitarán a las personas el ejercicio de los derechos enumerados en el presente Reglamento. A este efecto creará los procedimientos administrativos oportunos para que se puedan ejercer fácilmente los derechos de acceso, rectificación, cancelación y oposición.
2. Así, el Ayuntamiento y sus entidades vinculadas o dependientes quedan obligados mediante el presente Reglamento a:

a) Arbitrar un procedimiento específico para facilitar el ejercicio de estos derechos.
b) Poner a disposición de la ciudadanía modelos para el ejercicio de sus derechos de acceso, rectificación, cancelación y oposición, que estarán a disposición de las personas interesadas en el Registro General, en las oficinas de asistencia en materia de registro, en la sede electrónica del Ayuntamiento, en las subsedes, si procede, en los portales municipales de internet y en el portal de transparencia.

c) Informar y formar adecuadamente al personal que tenga acceso a los datos del fichero para que puedan atender adecuadamente a la ciudadanía en el ejercicio de sus derechos.
d) Incorporar progresivamente en las nuevas aplicaciones informáticas las funcionalidades que faciliten el ejercicio de los derechos de acceso, rectificación, cancelación u oposición, con el objeto de permitir a las personas interesadas la identificación de los procedimientos para el ejercicio de sus derechos.

Artículo 21. Contratación para la prestación de servicios que conlleven acceder a datos personales.

1. Cuando el Ayuntamiento y sus entidades vinculadas o dependientes faciliten el acceso a datos personales a una tercera persona o entidad para que realice un tratamiento concreto con ellos por encargo de la propia administración, no se considerará comunicación de datos.
2. Independientemente del coste de la prestación del servicio, el Ayuntamiento y sus entidades vinculadas o dependientes regularán la realización del tratamiento con la parte prestataria, mediante contrato por escrito en formato electrónico, cláusula administrativa particular en el mismo formato, o en cualquier otra forma, siempre que permita acreditar su celebración y contenido.
3. En el documento vinculante entre el Ayuntamiento o sus entidades vinculadas o dependientes y una tercera persona o entidad, quedarán expresamente recogidas las siguientes obligaciones para la empresa o entidad prestataria:

a) Asumir la obligación genérica de cumplimiento de lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y, expresamente, en lo indicado en su artículos 9 y 10, y en el Reglamento de desarrollo de la citada Ley Orgánica 15/1999, aprobado por Real Decreto 1720/2007, de 21 de diciembre, comprometiéndose explícitamente a informar y formar a su personal en las obligaciones que de tales normas dimanan.
b) Utilizar la información y datos de carácter personal que se le faciliten única y exclusivamente para la finalidad de realización de las actividades contempladas en el contrato de cesión de datos.
c) Tratar la información conforme a las instrucciones que consten o que se trasladen posteriormente.
d) Guardar el secreto profesional, tanto la empresa como el personal a su cargo, sobre todas las informaciones, documentos y asuntos a los que tenga acceso o conocimiento durante la vigencia del contrato, estando obligados a no hacer públicos o enajenar cuantos datos conozcan como consecuencia o con ocasión de su ejecución, incluso después de finalizar el plazo contractual.
e) Cumplir las medidas de seguridad y adoptar las medidas necesarias de índole técnica y organizativa que garanticen la seguridad de los datos personales que se le faciliten, conforme al nivel de seguridad

del fichero de que se trate, de tal manera que eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o de medio físico o natural.

f) No reproducir, ni comunicar, ni ceder a terceras personas o entidades información a la que tengan acceso durante la ejecución del contrato.

g) Poseer un Documento de Seguridad formalizado y documentado, en el que se determinen las medidas de índole técnica y organizativa que deben implantarse atendiendo a la naturaleza de los datos. A tal fin, la parte adjudicataria deberá aportar con anterioridad a que se produzca la cesión de datos, en su caso, una memoria descriptiva de las medidas que adoptará para asegurar la confidencialidad e integridad de los datos manejados y de la documentación facilitada, con indicación asimismo del nombre de la persona Responsable de la Seguridad en su empresa o entidad de esos datos y tratamientos, con especificación de su perfil profesional.

h) Informar al Ayuntamiento o a sus entidades vinculadas o dependientes, de modo inmediato, sobre cualquier sospecha relacionada con fallos o fugas del sistema de seguridad y protección de la información que pudiera ser detectado durante la ejecución del contrato.

i) Facilitar, en su caso, el control y auditoría por parte del Ayuntamiento o sus entidades vinculadas, mediante la aportación de la información que se le solicite e incluso, excepcionalmente, el acceso a los locales que se determinen. Incluso autorizar al Ayuntamiento y a sus entidades vinculadas o dependientes la posibilidad de utilizar registros de control en los ficheros facilitados.

j) No subcontratar la actividad, en todo o en parte, sin autorización expresa para ello. En este supuesto deberán recogerse por escrito en formato electrónico los datos que podrán facilitarse por la empresa adjudicataria a la empresa subcontratista y todas las obligaciones de ésta última, que serán como mínimo las de aquella, respecto del Ayuntamiento y sus entidades vinculadas o dependientes.

k) Borrar los datos o devolver el soporte informático en el que constan los datos personales que provienen de los ficheros que se le han facilitado, una vez prestados los servicios requeridos, sin conservar copia alguna del mismo, ni siquiera de seguridad, y sin que ninguna persona externa, física o jurídica, entre en conocimiento de los datos. Asimismo devolverá o destruirá todos los soportes magnéticos, soportes ópticos o cualquier otro tipo de soporte procesable, estando en cualquier caso a lo dispuesto en el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, en lo que concierne al borrado de información.

4. Con la finalidad de asegurar el cumplimiento de las prescripciones contempladas en el presente artículo, en los pliegos de cláusulas

administrativas generales o de condiciones técnicas, se recogerán las anteriores obligaciones para que sean asumidas por las personas participantes en los procedimientos de contratación administrativa.

5. Será necesario recoger en el contrato escrito que suscriban ambas partes, al menos, las cláusulas referidas a:

a) Acceso a locales donde se tratan datos personales.
b) Deber de confidencialidad de las personas que accedan a datos de carácter personal.
c) Cumplimiento de medidas de seguridad por parte de esas mismas personas.

Artículo 22. Tipos de fichero y niveles de seguridad.

1. De conformidad con lo dispuesto 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, de 13 de diciembre, de Protección de Datos de Carácter Personal, todos los ficheros que contengan datos de carácter personal deberán adoptar las medidas de seguridad calificadas como de nivel básico.
2. Los ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, los relativos a la administración tributaria, los de las mutuas de accidentes de trabajo y aquellos que permitan evaluar la personalidad deberán reunir, además de las medidas de nivel básico, las calificadas como de nivel medio.
3. Los ficheros que contengan datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual así como los que contengan datos recabados para fines policiales sin consentimiento de las personas afectadas y los que contengan datos derivados de actos de violencia de género deberán reunir, además de las medidas de nivel básico y medio, las calificadas de nivel alto.

Artículo 23. Funciones y obligaciones de las personas que tratan datos de carácter personal.

1. Todo el personal al servicio del Ayuntamiento o sus entidades vinculadas o dependientes que realice tratamientos de datos de carácter personal, de forma general o excepcional, deberá respetar la legislación y normativa aplicable al respecto, para lo que deberán aplicar de manera diligente lo establecido en la mencionada normativa y en el presente Reglamento.
2. Quienes tengan personas bajo su responsabilidad deberán formarlas debidamente en sus deberes y obligaciones respecto al tratamiento y protección de datos de carácter personal, prestando especial atención a la formación en la fase de acogida, cuando se incorporen por primera vez a sus equipos.
3. En el ámbito del Ayuntamiento y sus entidades vinculadas o dependientes, se identifican las siguientes figuras, como potenciales agentes en la protección de datos de carácter personal:

a) La Alcaldía, o en su caso, quien tenga delegadas las competencias en materia de Protección de Datos del Ayuntamiento de Cartagena, asumirá la máxima responsabilidad de la efectiva aplicación de la legislación y normativa.
b) El Responsable del Fichero: el Ayuntamiento se constituye como responsable último de todos los ficheros que contengan datos de carácter personal en sus instalaciones. Asimismo, le corresponde decidir sobre la finalidad, contenido y uso del tratamiento de datos de carácter personal. Para la realización de tareas operativas relacionadas con la seguridad de los ficheros la Alcaldía, o en su caso, quien tenga delegadas las competencias en materia de Protección de Datos del Ayuntamiento de Cartagena, designará, en caso de que delegue en otra, a la persona física que, de entre su personal, deba realizar las tareas de control de uno o varios ficheros, sin que dicha delegación de actividades suponga una exoneración de las responsabilidades que, en materia de seguridad de datos de carácter personal, corresponde al Ayuntamiento.
c) Responsable de Seguridad: la persona encargada de definir y velar por el cumplimiento de la estrategia global en materia de seguridad de la información en la administración y de la correcta adecuación de la misma a lo establecido en la legislación y normativa relativa a la protección de datos de carácter personal. Tiene atribuidas por la persona Responsable del Fichero la función de coordinar y controlar las medidas de seguridad aplicables. En el ejercicio de sus competencias podrá recabar la colaboración de Letrado Consistorial, Técnico de Administración General o Técnico en Administración Electrónica, pertenecientes al Grupo de Proyecto para la implantación de la Administración Electrónica, según Ordenanza Municipal de Administración Electrónica, a fin de asegurar la idoneidad de las propuestas o acciones que se deban realizar, en el ámbito jurídico.
d) Persona o entidad Encargada del tratamiento: la persona física o jurídica que, sola o conjuntamente con otros, trate datos personales por cuenta del Ayuntamiento y sus entidades vinculadas o dependientes. Cabe la posibilidad de que el Ayuntamiento o sus entidades vinculadas o dependientes contraten los servicios necesarios para llevar a cabo tratamientos de la información.
e) Persona colaboradora o coordinadora en materia de protección de datos: la persona que puede designar el Ayuntamiento con el encargo de coordinar, dinamizar y extender la nueva cultura de la protección de datos. Podrá coincidir o no con alguna de las figuras anteriores.

Artículo 24. Documento de Seguridad.

1. El Ayuntamiento implantará la normativa de seguridad mediante un Documento de seguridad de obligado cumplimiento para el personal con acceso a los datos de carácter personal y a los sistemas de

información, tanto de sus órganos como de sus entidades vinculadas o dependientes.

2. El Documento deberá contener, como mínimo, los siguientes aspectos:

a) Ámbito de aplicación del Documento, con especificación detallada de los recursos protegidos.
b) Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en la normativa vigente y en el presente Reglamento.
c) Funciones y obligaciones del personal.
d) Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.
e) Naturaleza de los datos sujetos a protección.
f) Procedimiento de notificación, gestión y respuesta ante las incidencias.
g) Procedimientos de realización de copias de respaldo y de recuperación de los datos.
h) Controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio Documento de Seguridad.
i) Medidas a adoptar cuando un soporte o documento tenga que ser transportado, desechado o reutilizado.

3. El Documento deberá mantenerse actualizado en todo momento y deberá ser revisado siempre que se produzcan cambios relevantes en el sistema de información o en la organización del mismo.

4. El contenido del Documento deberá adecuarse en todo momento a las disposiciones vigentes en materia de seguridad de los datos de carácter personal y ser coherente con la Política de Seguridad de la Información del Ayuntamiento.

Artículo 25. Comunicación de sus obligaciones a las personas con acceso a datos.

1. Las funciones y obligaciones de cada una de las personas con acceso a los datos de carácter personal y a los sistemas de información estarán claramente definidas y documentadas.
2. La persona Responsable del Fichero adoptará las medidas necesarias para que el personal conozca las normas de seguridad que afecten al desarrollo de sus funciones, así como las consecuencias en que pudiera incurrir en caso de incumplimiento.

Artículo 26. Sistemas de identificación y autenticación.

1. La persona Responsable del Fichero se encargará de que exista una relación actualizada de personas que tengan acceso autorizado a los sistemas de información y de establecer procedimientos de identificación y autenticación para dicho acceso.
2. Cuando el mecanismo de autenticación se base en la existencia de contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad.

3. Las contraseñas se cambiarán con la periodicidad que se determine en el Documento de Seguridad y mientras estén vigentes se almacenarán de forma ininteligible.
4. Se establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de toda persona usuaria que intente acceder a los sistemas de información y la verificación de que está autorizada para tal fin.
5. Las personas usuarias serán siempre personas físicas, identificadas de manera única, no permitiéndose los accesos de personas usuarias mediante cuentas o identificadores compartidos. Cada persona usuaria será responsable de todas las actuaciones que se realicen con su identificador.
6. Se limitará a tres veces la posibilidad de intentar reiteradamente el acceso no autorizado a los sistemas de información, bloqueándose los mismos tras estos tres intentos, de tal manera que el usuario tenga que contactar con el administrador del sistema para su desbloqueo, si procede.

Artículo 27. Control de acceso a aplicaciones informáticas.

1. Las personas usuarias tendrán acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones. Se establecerán mecanismos para evitar que una persona usuaria pueda acceder a datos o recursos con derechos distintos de los autorizados.
2. La relación de personas usuarias, a la que se refiere el artículo anterior del presente Reglamento, contendrá el acceso autorizado para cada una de ellas. Exclusivamente el personal autorizado para ello en el Documento de Seguridad podrá conceder, alterar o anular el acceso autorizado sobre los datos y recursos, conforme a los criterios establecidos en el Documento de Seguridad.

Artículo 28. Registro de accesos en ficheros de nivel alto.

1. De cada acceso se guardarán, como mínimo, la identificación de persona usuaria, la fecha y hora en que se realizó, el fichero al que se ha accedido, el tipo de acceso y si ha sido autorizado o denegado.
2. En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro al que se ha accedido.
3. Los mecanismos que permiten el registro de los datos detallados en los apartados anteriores estarán bajo el control directo de la persona Responsable de Seguridad, sin que se deba permitir, en ningún caso, la desactivación ni la manipulación de los mismos.
4. El período mínimo de conservación de los datos registrados será de dos años.
5. La persona Responsable de Seguridad se encargará de revisar periódicamente la información de control registrada y elaborará un

informe de las revisiones realizadas y de los problemas detectados, al menos una vez al mes.

Artículo 29. Acceso a locales donde estén ubicados los equipos con la información.

1. Solamente el personal autorizado en el Documento de Seguridad podrá tener acceso a los locales donde se encuentren ubicados los sistemas de información con datos de carácter personal.
2. Los locales donde estén ubicados los sistemas de información de nivel alto deberán estar dotados de un sistema de control de accesos que permita el acceso sólo a las personas autorizadas, disponiendo en todo momento de un registro de las personas y accesos realizados.

Artículo 30. Acceso a datos a través de la red.

La transmisión de datos de carácter personal a través de redes de telecomunicaciones se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni sea manipulada por terceras personas. Los datos sólo se mantendrán cifrados durante el proceso de transmisión.

Artículo 31. Régimen de trabajo en estaciones de trabajo, portátiles y en modalidad Cloud.

1. La ejecución de tratamientos de datos de carácter personal fuera de los sistemas informáticos del Ayuntamiento o de sus entidades vinculadas o dependientes, desde estaciones de trabajo o equipos portátiles particulares o propiedad de aquél o aquéllas, deberá ser autorizada expresamente por la persona Responsable del Fichero y, en todo caso, deberá garantizarse el nivel de seguridad correspondiente al tipo de fichero tratado y su cifrado.
2. En los casos en los que se haga uso de computación en Cloud, en cualquiera de sus modalidades, se estará a lo dispuesto en la Ordenanza de Administración Electrónica del Excelentísimo Ayuntamiento de Cartagena.

Artículo 32. Gestión de soportes.

1. Los soportes informáticos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen sólo a aquellos usuarios con acceso autorizado y deberán ser inventariados y etiquetarse para almacenarse en un lugar con acceso restringido al personal autorizado para ello en el Documento de Seguridad.
2. La salida de soportes informáticos que contengan datos de carácter personal, fuera de los locales en los que esté ubicado el fichero, únicamente podrá ser autorizada por la persona Responsable del Fichero.
3. Deberá establecerse un sistema de registro de entrada de soportes informáticos que permita, directa o indirectamente, conocer el tipo

de soporte, la fecha y hora, la persona emisora, el número de soportes, el tipo de información que contienen, la forma de envío y la persona responsable de la recepción que deberá estar debidamente autorizada.

4. Cuando un soporte vaya a ser desechado o reutilizado, se adoptarán las medidas necesarias para impedir cualquier recuperación posterior de la información almacenada en él, previamente a que se proceda a su baja en el inventario, adoptando para ello las medidas previstas en el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
5. Cuando los soportes se vayan a distribuir o vayan a salir fuera de los locales en que se encuentren ubicados los ficheros, como consecuencia de operaciones de mantenimiento, salvaguarda o de necesidades de trabajo, se adoptarán las medidas pertinentes encaminadas a evitar cualquier manipulación indebida de la información almacenada.

Artículo 33. Copias de respaldo y recuperación de los datos.

1. La persona Responsable del Fichero o, por delegación, la persona Responsable de Seguridad, se encargará de verificar la definición y correcta aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos.
2. Los procedimientos establecidos para la realización de copias de respaldo y para la recuperación de los datos deberán garantizar su reconstrucción en el estado en que se encontraban en el momento de producirse la pérdida o destrucción.
3. Deberán realizarse copias de respaldo de los ficheros con carácter diario, salvo que en dicho lapso no se hubiera producido ninguna actualización de los datos.
4. Deberá conservarse una copia de respaldo y de los procedimientos de recuperación de los datos en un lugar diferente de aquel en que se encuentren los equipos informáticos que los tratan, cumpliendo en todo caso las medidas de seguridad exigidas en el presente Reglamento.

Artículo 34. Ficheros temporales, copias de trabajo de documentos y pruebas con datos reales.

1. Los ficheros temporales o copias de documentos que se hubieran creado exclusivamente para la realización de trabajos temporales o auxiliares deberán cumplir el nivel de seguridad que les corresponda, con arreglo a la naturaleza de la información y, en su caso, de las finalidades de los mismos, en relación con la mayor o menor necesidad de garantizar la confidencialidad, integridad y disponibilidad de la información.

2. Todo fichero temporal o copia de trabajo así creado será borrado una vez que haya dejado de ser necesario para los fines que motivaron su creación.
3. Las pruebas anteriores a la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tipo de fichero tratado.

Artículo 35. Registro de incidencias.

1. El procedimiento de notificación y gestión de incidencias contendrá necesariamente un registro en el que se haga constar el tipo de incidencia, el momento en que se ha producido, la persona que realiza la notificación, a quién se le comunica y los efectos que se hubieran derivado de la misma.
2. Se deberán consignar en este registro los procedimientos realizados de recuperación de los datos, indicando la persona que ejecutó el proceso, los datos restaurados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación.
3. Será necesaria la autorización por escrito de la persona Responsable del Fichero para la ejecución de los procedimientos de recuperación de los datos.

Artículo 36. Circuito de datos en soporte papel y destrucción de copias.

1. Se evitará el uso de listados o copias impresas en papel que contengan datos personales. Cuando resulte imprescindible, se establecerá un sistema para que sólo las personas usuarias autorizadas tengan acceso a su contenido y evitar que la información sea accesible por personas no autorizadas.
2. En el supuesto de que sea necesario que la información en papel mencionada en el apartado anterior salga fuera de los locales administrativos se adoptarán las medidas necesarias para evitar un uso indebido de la misma.
3. Cuando los listados o copias impresas en papel dejen de ser necesarias se adoptarán las medidas necesarias para su destrucción.

Artículo 37. Auditorías.

1. Los sistemas de información e instalaciones de tratamiento de datos se someterán a una auditoría interna o externa anual, o en el supuesto de que se produzca un ciberincidente en los términos previstos en el "Reglamento de Evidencias Digitales del Excelentísimo Ayuntamiento de Cartagena", que verifique el cumplimiento del presente Reglamento y de los procedimientos e instrucciones vigentes en materia de seguridad de datos.
2. El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles al presente Reglamento y a la normativa vigente relativa a protección de datos de carácter personal,

identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias. Deberá, igualmente, incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y recomendaciones propuestas.

3. Los informes de auditoría serán analizados, en su caso, por la persona Responsable de Seguridad, quien comunicará las conclusiones al Responsable del Fichero para que se adopten las medidas correctoras adecuadas. Los informes de auditoría realizados quedarán a disposición de la Agencia Española de Protección de Datos.

Artículo 38. Actuaciones con respecto a ficheros no automatizados.

1. En lo que concierne a las actuaciones con respecto a los ficheros no automatizados, los dispositivos de almacenamiento de los documentos que contengan datos de carácter personal deberán disponer de mecanismos que obstaculicen su apertura. Igualmente se deberá identificar el tipo de información que contienen, ser inventariados y almacenarse en lugares controlados por el personal autorizado para ello en el Documento de Seguridad.
2. La persona Responsable del Fichero, de manera coordinada con el Jefe de Archivo, deberá establecer los procedimientos que deban seguirse en el archivo de los ficheros no automatizados. Dichos procedimientos estarán dirigidos a garantizar la correcta conservación de los documentos, la localización y consulta de la información y a posibilitar el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.
3. Mientras la información no se encuentre en el Archivo Municipal, por estar en revisión o tramitación, la persona que se encuentre a cargo de ella deberá custodiarla e impedir el acceso a la misma de personas no autorizadas.
4. Existirá para estos ficheros una persona Responsable de Seguridad con las mismas responsabilidades y funciones que para los ficheros automatizados.
5. Estos ficheros se someterán a una auditoria interna o externa al menos cada dos años.
6. El acceso a la documentación se limitará al personal autorizado en el Documento de Seguridad. Cuando existan múltiples personas, deberán establecerse mecanismos que permitan identificar los accesos.
7. El local en que se encuentre el fichero deberá estar dotado de puertas con llave o dispositivo equivalente, debiendo estar cerradas cuando no sea preciso el acceso a los documentos. Si ello no fuera posible, la persona Responsable de Seguridad hará un informe motivado proponiendo alternativas. En cualquier caso, los armarios, archivadores o elementos de almacenamiento deben tener sistemas que obstaculicen el acceso no autorizado.

8. La copia de documentos sólo podrá ser realizada por personal autorizado. Cuando se destruyan las copias, se hará mediante procedimientos que impidan su posterior recuperación.
9. En el traslado de estos ficheros deberán adoptarse medidas de seguridad que impidan el acceso a la documentación de personas no autorizadas, o la manipulación de la información o la detección de accesos no autorizados.

Artículo 39. Deber de secreto profesional.

1. Toda persona que intervenga en cualquier fase del tratamiento de los datos de carácter personal de ficheros está obligada al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aún después de finalizar su relación de servicio con el Ayuntamiento o sus entidades vinculadas o dependientes.
2. El incumplimiento del deber de secreto será sancionado de conformidad con lo previsto en la legislación vigente y traerá consigo, en su caso, las responsabilidades penales, disciplinarias y ante terceras personas o entidades que la misma establece.
3. Todas las personas al servicio del Ayuntamiento y de sus entidades vinculadas o dependientes están obligadas a guardar el secreto profesional en cuanto a los datos de carácter personal a los que tengan acceso.

Artículo 40. Obligaciones en las comunicaciones de datos.

1. Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a una tercera persona para el cumplimiento de fines directamente relacionados con las funciones legítimas del Ayuntamiento y de sus entidades vinculadas o dependientes y de la parte cesionaria, con el consentimiento expreso del interesado.
2. El consentimiento exigido en el apartado anterior no será preciso:

a) Cuando la cesión esté autorizada en una ley.
b) Cuando se trate de datos recogidos de fuentes accesibles al público.
c) Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceras personas o entidades. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.
d) Cuando la cesión se produzca entre el Ayuntamiento y sus entidades vinculadas o dependientes y otras administraciones públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos, con finalidades cuantitativas.
e) Cuando los datos hayan sido recogidos o elaborados por el Ayuntamiento o sus entidades vinculadas o dependientes con destino a otra administración, o cuando se realice para el ejercicio de competencias sobre las mismas materias.

f) Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia, que requiera acceder a un fichero, o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica.

3. Será nulo el consentimiento para la comunicación de los datos de carácter personal a una tercera persona, cuando la información que se facilite a la persona interesada no le permita conocer la finalidad a que destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquel a quien se pretenden comunicar.
4. El consentimiento para la comunicación de los datos de carácter personal tiene carácter revocable.
5. Aquella persona a quien se comuniquen los datos de carácter personal se obliga, por el solo hecho de la comunicación, a la observancia de las disposiciones legales y normativas objeto del presente Reglamento.
6. Si la comunicación se efectúa previo procedimiento de disociación, no será aplicable lo establecido en los apartados anteriores.

Artículo 41. Procedimiento para las cesiones de datos que requieran el consentimiento de la persona interesada.

En el caso de cesiones de datos al Ayuntamiento o a sus entidades vinculadas o dependientes que precisen del consentimiento de la persona interesada, se procederá de la siguiente forma:

a) El órgano solicitante remitirá su petición a la persona Responsable del Fichero, que valorará la oportunidad de la cesión así como su legalidad, sin perjuicio de que pueda recabar el asesoramiento jurídico de quien tenga atribuida dicha función en el Ayuntamiento.

b) La persona Responsable del Fichero remitirá la carta de condiciones, en formato electrónico, al órgano solicitante para que la firme mediante recibí y conforme.

c) La persona Responsable del Fichero comprobará la autorización prestada por las personas afectadas, debiendo solicitarles expresamente su consentimiento si fuera necesario, y llevará a cabo un sistema de marcado en las fichas personales generadas al efecto, donde consten en cada momento las cesiones realizadas, a fin de garantizar el efectivo ejercicio de los derechos de acceso, rectificación y cancelación de las personas interesadas.

d) La persona Responsable del Fichero comunicará los datos a la parte cesionaria en formato electrónico. Las cesiones realizadas serán reflejadas en el correspondiente registro electrónico de entradas y salidas del Documento de Seguridad del fichero.

Artículo 42. Procedimiento para las cesiones de datos que no requieran el consentimiento de la persona interesada.

En el caso de cesiones de datos que no precisen del consentimiento de la persona interesada, tales cesiones se llevarán a cabo mediante la

supervisión de la persona Responsable del Fichero. Sin carácter exhaustivo, se consideran cesiones de este tipo:

a) La cesión realizada a organismos judiciales y administrativos, de conformidad con las diferentes leyes aplicables, en el ejercicio de las funciones que tienen atribuidas y en los supuestos y condiciones establecidos en las citadas normas.
b) La cesión de datos personales pertenecientes a empleados del Ayuntamiento y de sus entidades vinculadas o dependientes realizada a quienes ostenten su representación sindical, en cumplimiento de la legislación sobre libertad sindical vigente en cada momento.
c) La cesión de datos de carácter personal relativos a la salud, si es necesaria para solucionar una urgencia que requiera acceder a un fichero automatizado, o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad y prevención de riesgos laborales vigente en cada momento.
d) La cesión que se efectúa previo procedimiento de disociación, es decir, de modo que la información que se obtenga no pueda asociarse a persona determinada o determinable.

Artículo 43. Utilización y tratamiento de datos del Padrón Municipal de Habitantes.

1. Las finalidades para las que se pueden utilizar los datos del Padrón Municipal de Habitantes son las establecidas al efecto en la Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local:

a) Determinar la población del municipio.
b) Constituir prueba de la residencia en el municipio y del domicilio habitual en el mismo.
c) Elaborar estadísticas sobre composición de familias, características económicas, nivel educativo, matrimonio, fecundidad y defunciones.

2. Los datos del Padrón Municipal de Habitantes se cederán a otras administraciones públicas que lo soliciten, sin consentimiento previo de la persona afectada, cuando les sean necesarios para el ejercicio de sus competencias, y exclusivamente para asuntos en los que la residencia o el domicilio sean datos relevantes, en los términos previstos en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
3. Los requisitos para la cesión de datos entre órganos del Ayuntamiento y con sus entidades vinculadas o dependientes son los mismos que los previstos para la cesión entre administraciones públicas. En consecuencia, cuando la cesión de datos del Padrón Municipal de Habitantes sea para el ejercicio de una competencia que corresponde al propio Ayuntamiento o a sus entidades vinculadas o dependientes, en la que el domicilio sea dato relevante, se comunicarán los mismos sin consentimiento de la persona interesada. Cuando concurra dicha circunstancia habrá de entenderse que existe compatibilidad de fines.

4. No ocurrirá lo mismo cuando los datos se cedan desde otros ficheros que no sean el del Padrón Municipal de Habitantes. En consecuencia, no podrá admitirse el uso compartido de los datos de un fichero en el que se recojan datos de carácter personal para la tramitación de un expediente administrativo, ni incluso a otro órgano del Ayuntamiento y a sus entidades vinculadas o dependientes, para el desarrollo de una competencia de ésta que no se encuentre expresamente contemplada entre las finalidades del fichero afectado, salvo que una Ley disponga otra cosa.

CAPÍTULO IV
Concurrencia del derecho a la protección de datos de carácter personal con otros derechos

Artículo 44. El derecho de acceso a la información.

El derecho a obtener información del Ayuntamiento o de sus entidades vinculadas o dependientes corresponde a toda persona por su condición de ciudadana, en los términos previstos en la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, codificados en la Ordenanza de Administración Electrónica del Excelentísimo Ayuntamiento de Cartagena.

Artículo 45. Publicidad y difusión de los actos administrativos.

1. Con carácter general, cuando deba procederse a la publicación o difusión por cualquier medio de los actos administrativos que deban darse a conocer a las personas interesadas o al público en general, y la información a suministrar contenga datos de filiación de personas concretas, se hará referencia a las mismas mediante las siglas de su nombre y apellidos, evitando, por tanto, su identificación directa.
2. En general, los boletines y diarios oficiales tienen la consideración de fuentes accesibles al público, por lo que los datos personales allí publicados pueden ser utilizados por terceras personas sin necesidad de solicitar el consentimiento de las personas interesadas, siempre que no se vulneren sus derechos y libertades fundamentales. Por ello, deberá reducirse al mínimo suficiente para cumplir su finalidad la información de carácter personal que se incluya en los documentos a publicar.
3. El Ayuntamiento y sus entidades vinculadas o dependientes podrán ofrecer a la ciudadanía información sobre el personal a su servicio, que integre tanto el puesto de trabajo como el número de teléfono y la cuenta de correo electrónico, con el fin de facilitar a la ciudadanía la identidad de la persona con quien deba contactar para realizar una determinada gestión.

Artículo 46. Publicidad en procesos de concurrencia competitiva y protección de datos.

En los procedimientos de concurrencia competitiva, tales como la selección y provisión de personal al servicio del Ayuntamiento y de sus entidades vinculadas o dependientes, la concesión de subvenciones, etc., se podrá proceder a la publicación de datos personales relativos a personas físicas identificadas o identificables haciendo uso de medios electrónicos, cuando así lo establezcan las normas reguladoras de cada procedimiento, a cuyo efecto se advertirá acerca de esta publicación en las bases de selección o en la convocatoria aprobadas.

Artículo 47. Petición de información por miembros de la Corporación y protección de datos.

1. Todas las personas que integran la Corporación tienen derecho a obtener de la Presidencia de la misma cuantos antecedentes, datos o informaciones obren en poder de los servicios del Ayuntamiento y sus entidades vinculadas o dependientes y resulten precisos para el desarrollo de su función de fiscalización y control de los órganos de gobierno de la misma, de conformidad con lo establecido en el artículo 77 de la Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local. En este sentido, el artículo 11.2 a) de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, en relación con el anterior, ofrece la cobertura suficiente para que a las personas que integran la Corporación se les puedan facilitar datos personales.
2. Deberán comunicarse sólo aquellos datos de carácter personal que resulten adecuados, pertinentes y no excesivos en relación con la concreta finalidad de gobierno o de fiscalización y control que las personas como miembros de la Corporación tengan atribuida.
3. Cuando la información a suministrar contenga datos de carácter personal, se deberá valorar, en primer lugar, si es posible proceder a su disociación sin que ello afecte al derecho de los miembros de la Corporación a recibir la información necesaria para el ejercicio de sus funciones de control de los órganos de gobierno del Ayuntamiento o de sus entidades vinculadas o dependientes. Y, cuando esta opción no fuera posible por comprometer la comprensión de la información que deba suministrarse, se comunicará a quien deba recibir la información el deber de reserva y confidencialidad que le incumbe, respecto de la información de carácter personal que conozca en el ejercicio de su cargo.
4. A la entrega de la documentación, se recordará a las personas que son miembros de la Corporación que deberán observar el deber de confidencialidad de la información y de los datos de carácter personal a los que accedan en el ejercicio de su cargo representativo, aún después de finalizado su mandato.
5. La valoración de cuáles resulten ser esos datos, así como el cumplimiento de los requisitos de la solicitud y su motivación, corresponde en exclusiva a los correspondientes órganos de gobierno del Ayuntamiento.

Artículo 48. Publicidad de los acuerdos de la Corporación.

Se deberán facilitar a las personas que lo soliciten copias y certificaciones acreditativas de los acuerdos de la Corporación, aunque podrán retirarse de las mismas los datos de carácter personal, particularmente los especialmente protegidos, o aquellos que puedan afectar al derecho a la intimidad personal y familiar.

DISPOSICIONES ADICIONALES

Primera. Formación.

El Ayuntamiento elaborará un plan anual de actividades informativas y acciones formativas dirigidas a todo su personal y de manera preferente, a quién trate datos personales y datos sensibles.

Asimismo, facilitará a su personal un decálogo que informe sobre los principios de la protección de datos, sus obligaciones y los derechos de la ciudadanía. El mismo se publicará en la intranet municipal y se adoptarán medidas para asegurar que todos los empleados públicos, especialmente los de nueva incorporación, tienen conocimiento del mismo.

Segunda. Glosario.

Los términos utilizados en el presente Reglamento se incorporarán al Glosario de Administración Electrónica previsto en la Ordenanza Municipal de Administración Electrónica.

DISPOSICIÓN TRANSITORIA ÚNICA
Formularios y modelos

Con carácter normativo, y en el plazo de tres meses desde la entrada en vigor del presente Reglamento, el Ayuntamiento aprobará los formularios y modelos necesarios para relacionarse física o electrónicamente, en materia de protección de datos, con los ciudadanos, los empleados municipales, otras administraciones y, en lo que proceda, con la Agencia Española de Protección de Datos.

DISPOSICIONES FINALES

Primera. Modificación y actualización del Reglamento.

Las modificaciones y actualizaciones al presente Reglamento derivadas de cambios en la legislación sobre la materia serán aprobadas por el órgano competente. En particular, antes del 25 de mayo del 2018 el Ayuntamiento y sus entidades vinculadas o dependientes deben ser conformes con lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de

datos), de lo cual debe quedar reflejo en la pertinente modificación del presente Reglamento.

Segunda. Entrada en vigor.

El presente Reglamento será objeto de aprobación y publicación de acuerdo con los trámites legales oportunos, se publicará en la sede electrónica del Ayuntamiento y en su portal de transparencia y entrará en vigor en el plazo establecido en el artículo 70.2 y 65 de la Ley 7/1985, de 2 de abril, reguladora de las Bases del Régimen Local, a partir de su publicación en el Boletín Oficial.

La Junta de Gobierno Local acuerda aprobar, por unanimidad, al anterior propuesta.

7. APROBACIÓN DE CÓDIGOS DE DIRECTORIO DIR3 PARA LA IMPLANTACIÓN DE LA ADMINISTRACIÓN ELECTRÓNICA EN EL AYUNTAMIENTO DE CARTAGENA.

El artículo 9 del Real Decreto Legislativo 4/2010, de 8 de enero, por el que se aprueba el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica, establece lo siguiente:

> *"Artículo 9. Inventarios de información administrativa.*
> *1. Las Administraciones públicas (…) mantendrán una relación actualizada de sus órganos administrativos y oficinas de registro y atención al ciudadano, y sus relaciones entre ellos. Dichos órganos y oficinas se codificarán de forma unívoca y esta codificación se difundirá entre las Administraciones públicas.*
> *2. Cada Administración pública regulará la forma de creación y mantenimiento de este Inventario, que se enlazará e interoperará con el Inventario de la Administración General del Estado en las condiciones que se determinen por ambas partes y en el marco de lo previsto en el presente Real Decreto; en su caso, las Administraciones públicas podrán hacer uso del citado Inventario centralizado para la creación y mantenimiento de sus propios inventarios. (...)"*

El Inventario de la Administración General del Estado queda implementado mediante el Directorio Común (DIR3), proporcionando la relación jerárquica de la estructura de las Administraciones con codificación única, y actualizado de forma corresponsable por todas las Administraciones participantes.

El mantenimiento de los códigos y la gestión del ciclo de vida de la información del Directorio es esencial, entre otros, para conformar los metadatos asociados a las Normas Técnicas de Interoperabilidad de

Expediente Electrónico, e Intercambio de Datos entre Entidades Registrales (SICRES 3.0), en particular:

. Los Expedientes Electrónicos, incluyen el código de órgano en su nombre de fichero y en sus metadatos.
. La información de los Asientos Registrales está asociada al código de la Oficina de Registro que los emite, y al Código de Órgano de la Unidad de Tramitación.
. Las Facturas Electrónicas necesitan la identificación de la unidad tramitadora y el órgano gestor, identificados con su Código de Órgano.

Además, la Resolución de de 28 de junio de 2012, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Norma Técnica de Interoperabilidad de Relación de modelos de datos, (Boletín Oficial del Estado, núm. 178 de 26 de julio de 2012, páginas 53793 a 53807), establece que:

"VIII.2 La codificación de Unidades Orgánicas y Oficinas de la Administración en los modelos de datos aplicará las establecidas en el Directorio Común de Organismos y Oficinas, que será gestionado por el Ministerio de Hacienda y Administraciones Públicas y alimentado por todos los órganos de la Administración pública o Entidades de Derecho Público vinculadas o dependientes de aquélla. El Centro de Interoperabilidad Semántica publicará toda la documentación de integración, procedimientos de colaboración, y definición de atributos de la información del Directorio, teniendo en cuenta lo recogido en esta norma sobre intercambio de modelos de datos. Asimismo, dicho Centro publicará y mantendrá actualizada una relación de las fuentes colaboradoras y un enlace a la aplicación de gestión del Directorio Común."

La Dirección de Tecnologías de la Información y las Comunicaciones (DTIC) con el fin de dar respuesta a los requisitos del ENI, gestiona el "Directorio Común de Unidades Orgánicas y Oficinas", para proporcionar un Inventario unificado y común a todas las Administraciones, que incluye la relación de las unidades orgánicas y sus oficinas asociadas, y facilita el mantenimiento distribuido y corresponsable de la información.

La obligación de creación y publicación de la relación actualizada de órganos administrativos y oficinas de registro y atención al ciudadano, es común a todas las Administraciones Públicas incluidas en el artículo 2 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, en el que se incluyen tanto el Ayuntamiento de Cartagena como sus organismos autónomos dependientes así como las entidades de derecho público vinculadas a esta entidad local.

Por un lado, del artículo 9 del RD Legislativo 4/2010, se deriva que deben estar incluidos en este Directorio, tanto los órganos administrativos como las oficinas de registro y atención al ciudadano. El Modelo de Codificación del Directorio Común del Esquema Nacional de Interoperabilidad en su versión última de 8 de agosto de 2016, elaborado por la Dirección de Tecnologías de la Información y de las Comunicaciones del Ministerio de Hacienda y Administraciones Públicas, establece que los órganos administrativos se jerarquizan en unidades orgánicas, entendiendo como tales, en el marco del Directorio Común, cualquier unidad administrativa que realice un ejercicio de funciones con trascendencia jurídica. No obstante, aparte de las unidades orgánicas y las oficinas de registro y atención al ciudadano, el Directorio Común, debe contener así mismo las unidades no orgánicas. En este sentido, el apartado 4.2 de la Guía de Buenas Prácticas del Directorio Común elaborado por la DTIC en su versión de 7/07/2016, establece que, debido al crecimiento del DIR3: *"surge la necesidad de introducir nuevos tipos de unidades que no cumplen con la estructura de las unidades orgánicas, por este motivo se constituye el repositorio de unidades no orgánicas. La información introducida para estas unidades debe estar sujeta a una serie de normas de calidad, con el fin de que la información sea clara, concreta, de fácil comprensión y pueda ser explotada de forma eficiente.*

Según la DTIC: *"Se entiende por unidad no orgánica, todas aquellas unidades de rango inferior o independiente que queden excluidas del ámbito de una Unidad Orgánica.*

Dentro de las unidades no orgánicas existen 2 tipos:

UGEP

El Punto General de Entrada de Facturas Electrónicas de la AGE (FACe) surge como respuesta a la Ley 25/2013, de 27 de diciembre, de impulso de la factura electrónica y creación del registro contable de facturas en el Sector Público, que determina la obligatoriedad por parte del proveedor que presta servicios a cualquier Administración Pública, de presentar facturas ante un registro administrativo, en los términos previstos en el artículo 16 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas

En la mencionada ley se crean los registros contables de facturas (RCF) en las entidades públicas de su ámbito de aplicación, siendo regulados los requisitos funcionales y técnicos del registro contable de facturas mediante la Orden Ministerial HAP/492/2014, de 27 de marzo.

La Disposición Adicional Tercera de esta Orden Ministerial

HAP/492/2014, de 27 de marzo, determina que las facturas que se expidan a partir de la entrada en vigor de esta Orden ajustarán la codificación de los órganos administrativos que participen en la tramitación de las mismas a la establecida en el Directorio Común de Unidades Orgánicas (DIR3) gestionado por la Secretaría de Estado de Administraciones Públicas.

Por tanto para que FACe pueda redirigir adecuadamente las facturas al registro contable de facturas de la oficina contable correspondiente y para que posteriormente este RCF pueda hacer lo propio para ponerlas a disposición de la unidad tramitadora que corresponda es necesario que las unidades que participan en la tramitación de las facturas, es decir oficina contable, unidad tramitadora y órgano gestor, estén dadas de alta en el Directorio Común de Unidades Orgánicas, que generará un código único (código DIR3) para cada unidad, y deberán activarse además estas unidades en FACe.

Para todas aquellas unidades no orgánicas que tengan funciones de gestión económico-presupuestarias (ej. Caja Pagadora), se ha previsto en DIR3 un nuevo tipo específico de unidad, denominado Unidad de Gestión Económica Presupuestaria (UGEP).

Entidades Colaboradoras
Con motivo de la aprobación de la Ley de medidas de reforma administrativa en el ámbito de la Administración de Justicia y del Registro Civil. (121/000101), se precisa que figuren en DIR3 las ventanillas únicas correspondientes a los centros sanitarios que permiten la remisión telemática de los nacimientos al Registro Civil, creando para ello en DIR3 un nuevo tipo denominado Entidades Colaboradoras (EECC)"

El Ayuntamiento de Cartagena, tiene asignado el código LO1300161 en el Directorio Común de unidades orgánicas que gestiona la Dirección de Tecnologías de la Información y las Comunicaciones (DTIC) y la publicación de las siguientes unidades orgánicas:

L01300161-Ayuntamiento de Cartagena
- LA0001483-Administración y Servicios Generales
  - LA0001499-Registro General
- LA0003527-Agencia de Desarrollo Local y Empleo
- LA0006330-Alcaldía
  - LA0007004-Junta Vecinal de Alumbres
  - LA0007002-Junta Vecinal de el Albujón
  - LA0007013-Junta Vecinal de el Algar
  - LA0007007-Junta Vecinal de el Llano del Beal
  - LA0007006-Junta Vecinal de Isla Plana

LA0007003-Junta Vecinal de la Aljorra
LA0007009-Junta Vecinal de la Palma
LA0007012-Junta Vecinal de la Puebla
LA0007005-Junta Vecinal de los Dolores
LA0007008-Junta Vecinal de los Molinos Marfagones
LA0007010-Junta Vecinal de Perín
LA0007011-Junta Vecinal de Pozo Estrecho
LA0006626-Secretaría
LA0006842-Servicios Jurídicos
LA0004484-Archivo
LA0005040-Área de Infraestructuras
LA0005041-Unidad Administrativa de Infraestructuras
LA0003537-Carmen Conde
LA0006926-Consejo Económico-Administrativo
LA0006625-Coordinación de Educación
LA0008362-Coordinador de Educación
LA0006617-Dirección de Servicios Sociales
LA0005809-Director Económico y Presupuestario
LA0007016-Jefe de Contratación y Compras
LA0008009-Responsable de Compras y Almacenes
LA0007017-Responsable de Contratación
LA0005810-Patrimonio
LA0003534-Fundación Rifa Benéfica Casa Niño
LA0003540-Instituto Municipal Servicios Litoral
LA0008042-Intervención
LA0006079-Jefatura de Descentralizacion
LA0006080-Unidad Administrativa de Descentralizacion
LA0006620-Jefatura de Recursos Humanos
LA0006618-Jefatura de Servicios Administrativos Generales
LA0006619-Jefatura de Población y Estadística
LA0006621-Jefatura del Área de Urbanismo
LA0006622-Jefatura del Servicio Jurídico Administrativo de Intervención Urbanística
LA0006678-Disciplina Ambiental
LA0006680-Disciplina Urbanística
LA0006682-Licencias de Actividad
LA0006683-Licencias Urbanísticas
LA0006624-Jefatura del Servicio Jurídico de Gestión Urbanística
LA0006623-Jefatura del Servicio Jurídico de Planeamiento y Medio Ambiente
LA0006681-Seguridad en la Edificación
LA0008502-Servicio de Documentación e Información Urbanística
LA0008504-Documentación Urbanística
LA0008503-Información Urbanística
LA0006679-Nuevas Tecnologías Urbanismo

LA0006704-Urbanización y Obras
LA0006628-Jefe de Tráfico y Ocupación de la Vía Pública
LA0006630-Multas
LA0006629-Responsable de Mercadillos y Venta Ambulante
LA0008668-Responsable de Ocupación de la Vía Publica
LA0005811-Nuevas Tecnologías
LA0005812-Oficina de Gobierno
LA0007473-Oficina de Transparencia
LA0003535-Organismo Gestión Recaudatoria
LA0006675-Órgano de Gestión Tributaria
LA0006677-Inspección Tributaria
LA0006676-Unidad Administrativa del Órgano de Gestión Tributaria
LA0007499-Recursos Humanos
LA0007666-Formación
LA0007667-Gestión de Prevención de Riesgos Laborales
LA0007843-Jefe de Nóminas y Seguridad Social
LA0007844-Jefe de Provisión y Selección
LA0007668-Relaciones Laborales, Organización e Inspección
LA0007669-Responsable Administrativo de Gestión de Personal
LA0007474-Sanidad Calidad de Vida
LA0008632-Subinspector Jefe de la Policía Local
LA0001482-Tesorería
LA0001852-Registro Facturas
LA0008159-Vicealcaldía
LA0008160-Comercio

A la vista de lo expuesto, es necesario la modificación del listado de unidades orgánicas que figura publicado en la DTIC para su adaptación al marco del Directorio Común y a la división del Ayuntamiento de Cartagena y sus organismos autónomos en unidades orgánicas, oficinas de registro y de atención al ciudadano y unidades no orgánicas (UGEP), conforme a la estructura orgánica municipal que se deriva del Decreto de creación de Áreas de Gobierno de fecha 16 de junio de 2015, y a la organización jerarquizada de las distintas unidades administrativas creadas a raíz del citado Decreto para la gestión de actuaciones administrativas con trascendencia jurídica.

Visto el informe emitido por la Jefe de Servicios Administrativos Generales de fecha 28 de noviembre de 2016 y el informe emitido por la Jefe de Organización e Inspección de fecha 16 de diciembre de 2016, se adjunta a continuación, el listado de los Códigos DIR3 de las unidades orgánicas, oficinas de registro y atención al ciudadano y unidades no orgánicas del Ayuntamiento de Cartagena, incluyéndose en el listado de oficinas de registro y atención al ciudadano, el registro auxiliar del ADLE de pronta creación:

UNIDADES ORGÁNICAS

L01300161-Ayuntamiento de Cartagena

LA0006330-Alcaldía
- LA0009079-Gabinete de Alcaldía-presidencia.
- LA0006626-Secretaría General del Pleno
- LA0005812-Oficina de Gobierno Municipal
- LA0006842-Asesoría Jurídica

LA0008159-Vicealcaldía
- LA0009080-Estrategia Económica
- LA0009081-Turismo
- LA0003527-Agencia de Desarrollo Local y Empleo
- LA0008160-Innovación, Empresa y Comercio
- LA0009082-Litoral

LA0009083-Interior
- LA0007499-Recursos Humanos
  - LA0007666- Formación
  - LA0007667- Gestión de Prevención de Riesgos Laborales
  - LA0007844- Provisión, Promoción y Selección
  - LA0007668-Relaciones Laborales, Organización e Inspección
- LA0004484-Archivo Municipal
- LA0005811-Nuevas Tecnologías
- LA0001483-Servicios Generales
  - LA0006619-Estadística y Población
- LA0008632-Policía Local
- LA0006628-Sanciones de Tráfico y Ocupación de Vía Pública
  - LA0006630-Multas
  - LA0006629-Mercadillos y venta ambulante
  - LA0008668-Ocupación de la vía pública
- LA0009084-Protección Civil
- LA0009085-Servicio de Extinción de Incendios
- LA0009086-Responsabilidad Patrimonial

LA0009087-Hacienda
- LA0005809-Oficina económica y presupuestaria
  - LA0007016-Contratación y compras
    - LA0008009-Compras y Almacenes
    - LA0007017-Contratación
  - LA0006926-Consejo Económico-Administrativo
  - LA0005810-Patrimonio
- LA0008042-Intervención
- LA0001482-Tesorería
- LA0006675-Gestión Tributaria
  - LA0006677-Inspección de Rentas

LA0003535-Organismo Autónomo de Gestión Recaudatoria

LA0006621-Urbanismo
- LA0008502-Documentación e Información
  - LA0008504-Documentación Urbanística
  - LA0008503-Información Urbanística
  - LA0006679-Nuevas Tecnologías Urbanismo
- LA0009088-Planeamiento Urbanístico
- LA0009089-Medio Ambiente
- LA0006624-Gestión Urbanística
- LA0006704-Urbanización y obras
- LA0009090-Servicio de Intervención Urbanística
  - LA0006683-Licencias urbanísticas
  - LA0006680-Disciplina urbanística
    - LA0006681-Seguridad en la edificación
  - LA0006682-Licencias de Actividad
  - LA0006678-Disciplina Ambiental
- LA0009091-Casco Antiguo Cartagena

LA0005040-Infraestructuras
- LA0005041-Unidad Administrativa de Infraestructuras
- LA0009092-Control de Servicios
- LA0009093-Arquitectura y Rehabilitación
- LA0009094-Obras y Proyectos de Ingeniería
- LA0009095-Conservación

LA0007473-Transparencia

LA0006079-Descentralización y Participación Ciudadana
- LA0007004-Junta Vecinal de Alumbres
- LA0007002-Junta Vecinal de El Albujón-Miranda
- LA0007013-Junta Vecinal de El Algar
- LA0007007-Junta Vecinal de El Llano del Beal
- LA0007006-Junta Vecinal de Isla Plana
- LA0007003-Junta Vecinal de La Aljorra
- LA0007009-Junta Vecinal de La Palma
- LA0007012-Junta Vecinal de La Puebla-La Aparecida
- LA0007005-Junta Vecinal de Los Dolores
- LA0007008-Junta Vecinal de Molinos Marfagones
- LA0007010-Junta Vecinal de Perín
- LA0007011-Junta Vecinal de Pozo Estrecho
- LA0006080-Unidad administrativa de descentralización
- LA0009096-Unidad Técnica de descentralización
- LA0009097-Distrito nº 1
- LA0009098-Distrito nº 2
- LA0009099-Distrito nº 3
- LA0009100-Distrito nº 4

LA0009101-Distrito nº 5
LA0009102-Distrito nº 6
LA0009103-Distrito nº 7
LA0009104-Comisión de sugerencias y reclamaciones
LA0009105-Comisión de participación ciudadana
LA0009106-Comisión de coordinación de juntas
LA0009107-Consejo Social

LA0009108-Festejos

LA0006617-Servicios Sociales
LA0009109-Centro Municipal de Servicios Sociales I
LA0009110-Centro Municipal de Servicios Sociales II
LA0009111-Atención a personas mayores y discapacitados
LA0009112-Prevención y Promoción Social
LA0009113-Inmigración y cooperación al Desarrollo
LA0003534-Fundación Rifa Benéfica Casa del Niño

LA0009114-Consumo

LA0007474-Sanidad Calidad de Vida
LA0009115-Laboratorio municipal

LA0009116-Cultura
LA0009117-Universidad Popular
LA0009118-Museos
LA0009119-Bibliotecas
LA0003537-Patronato Municipal Carmen Conde-Antonio Oliver
LA0009132-Patrimonio Histórico-Arqueológico

LA0006625-Educación
LA0009133-Escuelas Infantiles
LA0009121-Gestión Educativa y Atención Psicopedagógica
LA0009122-Reeducación, Logopedia y Psicomotricidad
LA0009123-Promoción Educativa
LA0009124-Infraestructuras y conservación de centros escolares

LA0009125-Igualdad

LA0009126-Juventud
LA0009127-Ocio y participación
LA0009128-Programas Especiales
LA0009129-Informajoven

LA0009130-Deportes

OFICINAS DE REGISTRO Y DE ATENCIÓN AL CIUDADANO

O00011054-Registro General y Atención al ciudadano edificio San Miguel
O00011080-Registro Auxiliar ADLE
O00011055-Registro Auxiliar de Bomberos
O00011056-Registro Auxiliar de Cultura
O00011057-Registro Auxiliar de Deportes
O00011058-Registro Auxiliar de Educación
O00011059- Registro Auxiliar de Juventud
O00011085-Registro Auxiliar Oficina de Sanciones de Tráfico
O00011086-Registro Auxiliar de Policía
O00011087-Registro Auxiliar del Pleno
O00011060-Registro Auxiliar de Servicios Sociales
O00011061-Registro Auxiliar de Urbanismo
O00011062-OMITA Alumbres
O00011063-OMITA Barrio Peral
O00011064-OMITA Canteras
O00011065-OMITA El Albujón
O00011079-OMITA El Algar
O00011066-OMITA EL Llano del Beal
O00011067-OMITA Isla Plana
O00011068-OMITA La Aljorra
O00011069-OMITA La Manga
O00011070-OMITA La Palma
O00011071-OMITA La Puebla
O00011072-OMITA Los Belones
O00011073-OMITA Los Dolores
O00011071-OMITA Los Urrutias
O00011072-OMITA Miranda
O00011076-OMITA Molinos Marfagones
O00011077-OMITA Perín
O00011078-OMITA Pozo Estrecho

UNIDADES NO ORGANICAS (UGEP)
GE0012474-Registro de facturas

En virtud de lo expuesto, y siendo de obligado cumplimiento publicar en la sede electrónica municipal los códigos de unidades DIR3 para el correcto direccionamiento de las solicitudes de los ciudadanos, y su remisión a la Dirección de Tecnologías de la Información y de las Comunicaciones para su publicación y conocimiento del resto de Administraciones Públicas, es por lo que, cumpliendo con los requisitos establecidos en la normativa en vigor, particularmente en el 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 y las Normas Técnicas de Interoperabilidad que lo desarrollan, y en cumplimiento de la obligación que nos exige a las Administraciones Públicas la entrada en vigor de las Leyes 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones

Públicas y 40/2015, de 1 de octubre, del Régimen Jurídico del Sector Público, en el ejercicio de las competencias que tengo atribuidas, elevo a la Junta de Gobierno Local la siguiente PROPUESTA para que, previa deliberación adopte, si lo considera procedente, el siguiente **ACUERDO:**

PRIMERO: La aprobación de los Códigos DIR3 de las unidades orgánicas, oficinas de registro y atención al ciudadano y unidades no orgánicas del Excmo. Ayuntamiento de Cartagena relacionadas en el contenido de la presente resolución.

SEGUNDO: Su publicación en la sede electrónica municipal.

TERCERO: Ordenar la tramitación correspondiente para su inclusión y publicación en el "Directorio Común de Unidades Orgánicas y Oficinas", que gestiona la Dirección de Tecnologías de la Información y las Comunicaciones (DTIC), como inventario común y unificado a todas las Administraciones Públicas con el fin de dar respuesta a los requisitos del Esquema Nacional de Interoperabilidad.

No obstante, la Junta de Gobierno Local resolverá lo que mejor proceda.= Cartagena, a 22 de diciembre de 2016.= EL CONCEJAL DELEGADO DEL ÁREA DE HACIENDA E INTERIOR.= Firmado, Francisco Aznar García, rubricado.

La Junta de Gobierno Local acuerda aprobar, por unanimidad, al anterior propuesta.

ÁREA DE GOBIERNO DE URBANISMO E INFRAESTRUCTURAS

Propuestas presentadas por el Alcalde Presidente tramitadas por el siguiente Servicio:

URBANISMO

8. ADQUISICIÓN DE FINCA EN CALLE CUATRO SANTOS, N.º 3 Y 5, CALIFICADA COMO EQUIPAMIENTO ADMINISTRATIVO.

El Alcalde-Presidente, en cuanto titular del Área de Urbanismo e Infraestructuras, ha conocido del expediente de adquisición de la finca sita en calle Cuatro Santos, n.º 3 y 5 de Cartagena, así como de la propuesta de resolución de la Jefe del Servicio Jurídico de Gestión Urbanística, conforme lo siguiente:

Por los propietarios de la finca sita en calle Cuatro Santos, n.º 3 y 5, de Cartagena, representados por [redacted], se ha presentado

escrito de ofrecimiento de dicha finca para su adquisición, dado que se encuentra calificado como Equipamiento Dotacional.

La finca que se ofrece es la que se describe a continuación:
"URBANA: Edificio marcado con los números tres y cinco de la calle Cuatro Santos, de Cartagena, asentado sobre una superficie de doscientos veintidós metros y treinta decímetros cuadrados. Dicho edificio presenta una forma escalonada, es decir, consta de planta baja y plantas de piso primero, segundo, tercero y cuarto, en su zona frontal, o calle Cuatro Santos, y de planta baja y planta de piso primero y segundo a la denominada calle o callejón del Mico. La planta baja y las plantas de piso primero y segundo tienen una superficie construida, cada una de ellas de doscientos veintidós metros cuadrados y las plantas de piso tercero y cuarto de ciento cincuenta metros cuadrados cada una de ellas. La superficie total construida en la edificación es por tanto de novecientos sesenta y seis metros cuadrados. Las plantas baja o de calle y primera, segunda y tercera o de piso, están destinadas a hotel de una estrella con todas las dependencias necesarias para ello, y la planta cuarta o de piso a residencia, distribuida en varias dependencias. Para la circulación vertical dispone de ascensor y escalera general, mas otra escalera que llega hasta la altura de la tercera planta. El inmueble está provisto de los servicios de energía eléctrica, alcantarillado, agua potable, encintado de aceras, alumbrado público, etc. linda en su conjunto, al frente o sur, la calle de su situación denominada Cuatro Santos; este o derecha entrando, propiedad de doña Teresa Arnau; norte o espalda, otra de doña Carmen Vallejo y oeste o izquierda, calle o callejón del Mico.
Inscripción: Finca registral n.º [redacted], Tomo [redacted], libro [redacted] folio [redacted]
Sección del Registro de la Propiedad n. [redacted] de [redacted].
Título: Le pertenece a [redacted]".
Título: Lo adquirieron los titulares en virtud de escritura de herencia otorgada al fallecimiento de [redacted], de fecha 25 de abril de 2006, ante el Notario de Cartagena D. Pedro E. Díaz Trenado, n.º 2335 de su protocolo.
Cargas: Consta una hipoteca de Caja de Ahorros de Murcia por importe de 36.060,73.- euros de principal, 9015,18 euros para costas y gastos, 4327,29 euros para intereses ordinario, 14.424,29 euros para intereses de demora y la cantidad de 1803,04 euros para prestaciones accesorias, otorgada en fecha 23 de noviembre de 1994.
Manifiestan los propietarios que dicha hipoteca se encuentra en trámites de cancelación.
Referencia catastral: [redacted]

Consta en el expediente informe técnico de valoración, emitido por la Arquitecta Municipal, de fecha 22 de diciembre de 2016, en el que consta

que la finca se encuentra clasificada por el Plan Especial de Protección del Casco Histórico (PEPCH), como suelo urbano consolidado, y calificado con uso DOTACIONAL ADMINISTRATIVO. Se encuentra situado en espacio urbano de interés, afectado por el entorno de protección de BIC, zona A., siendo la valoración, de 505.609,00.-€ (Quinientos Cinco Mil Seiscientos Nueve Euros).

Consta en el expediente escrito de conformidad de los propietarios con el precio indicado.

Consta asímismo, documentos de retención de crédito n.° RC2016.2.0026578.000 y n.° A2016.2.0026580.000, que suman el importe de la adquisición.

Por ello el Alcalde Presidente, ha resuelto proponer a la Junta de Gobierno Local, en virtud de las competencias que corresponden a esta, conforme al art. 127-1° D, de la Ley 7/1985 de 2 de abril, Reguladora de las Bases de Régimen Local, la adopción del siguiente acuerdo:

Primero.- Aprobar la adquisición de la finca descrita anteriormente, registral 16048, por el precio de 505.609.-€ (Quinientos Cinco Mil Seiscientos Nueve Euros), para su incorporación al patrimonio municipal.

Segundo.- Todos los gastos derivados del otorgamiento de la escritura de adquisición, serán por cuenta del Ayuntamiento. En cuanto a los impuestos, la operación resulta exenta por tratarse de una adquisición por expropiación.

Cartagena, 23 de diciembre de 2016.= EL ALCALDE-PRESIDENTE.= Firmado, José López Martínez, rubricado.

La Junta de Gobierno Local acuerda aprobar, por unanimidad, al anterior propuesta.

9. MODIFICACIÓN DE LAS CONDICIONES DE PAGO EN RELACIÓN CON LA EXPROPIACIÓN DE LAS PARCELAS 30.1 Y 30.2 INCLUIDA EN EL ÁMBITO DE SISTEMA GENERAL VIARIO DENOMINADO ACCESO NORTE.

El Alcalde-Presidente, en cuanto titular del Área de Urbanismo e Infraestructuras, ha conocido del expediente de expropiación de Parcela n° 12 incluida en el ámbito del Sistema General denominado Eje Transversal, así como de la propuesta de resolución de la Jefe del Servicio Jurídico de Gestión Urbanística, conforme lo siguiente:

"Por acuerdo de la Junta de Gobierno Local de fecha 14 de enero de 2005, se aprueba el inicio de expediente para la obtención de los terrenos calificados como Sistema General Viario Acceso Norte de Cartagena, entre los que se encuentra las parcelas nº 30.1 y 30.2, propiedad de [redacted].

En dicho proyecto se preveía que el justiprecio para las fincas de referencia se efectuaría mediante la asignación de aprovechamiento urbanístico en el sector BP1.

A tal efecto, en fecha 17 de mayo de 2005, se suscribe Acta de Pago y Ocupación de los terrenos objeto de expropiación, que tienen una superficie de 593,00 m2., cada una de las parcelas siendo el justiprecio de 23.677,00.-€, para cada una de ellas, materializados de la siguiente forma:

- La cantidad de 17.197,00.-€ mediante aprovechamiento urbanístico en el Sector BP1, para cada una de las parcelas.
- El importe de 6.480,00.-€, correspondiente al arbolado de cada una de las fincas, que se abonan mediante transferencia bancaria.

Resultando que por los propietarios expropiados se presenta escrito en fecha 19 de diciembre de 2016, solicitando el pago en metálico de la cantidad correspondiente al aprovechamiento urbanístico en el Sector BP1, valorados en 34.394,00.-€ para las dos parcelas, a razón de 17.197,00.-€ para cada una de ellas, dado que dicho planeamiento se encuentra a día de la fecha, sin desarrollar.

De la totalidad del justiprecio, 23.677,00.-€, se ha descontado el importe de 6.480,00.-€, que ya fué abonado por este Ayuntamiento a cada uno de los titulares mediante transferencia bancaria.

Consta en el expediente documento de retención de crédito n.º 2016.2.0026497.000, por el importe de 34.394,00.-€.

Considerando que los terrenos expropiados correspondiente a las Parcelas 30.1 y 30.2, de 1.186 m2., se encuentran inscritos a favor del Ayuntamiento, en el Registro de la Propiedad n[redacted], con los números de finca [redacted], obrante al folio [redacted], Libro [redacted] de la [redacted] Sección y [redacted], obrante en el folio [redacted] libro [redacted] de la [redacted] Sección.

Por ello el Alcalde Presidente, ha resuelto proponer a la Junta de Gobierno Local, en virtud de las competencias que corresponden a esta, conforme al art. 127-1° D, de la Ley 7/1985 de 2 de abril, Reguladora de las Bases de Régimen Local, la adopción del siguiente acuerdo:

Primero.- Modificar las condiciones de pago del justiprecio de las fincas registrales [redacted], que figuran en el Acta de de Pago y Ocupación suscrita el 17 de mayo de 2005, y se abone la cantidad pendiente de materializar en dicha Acta, que asciende a 34.394,00.-€ mediante su pago en metálico.

Segundo.- Facultar al Director General de Urbanismo para formalizar el presente acuerdo mediante el otorgamiento de los citados documentos o cuantos fueren precisos.

Cartagena, 21 de diciembre de 2016.= EL ALCALDE-PRESIDENTE.= Firmado, José López Martínez, rubricado.

La Junta de Gobierno Local acuerda aprobar, por unanimidad, al anterior propuesta.

ÁREA DE GOBIERNO DE CULTURA Y PATRIMONIO

Propuestas presentadas por el Concejal Delegado del Área de Cultura y Patrimonio tramitadas por los siguientes Servicios:

PATRIMONIO ARQUEOLÓGICO

10. **SUBVENCIÓN A LA FUNDACIÓN TEATRO ROMANO DE CARTAGENA.**

En relación con la modificación del Presupuesto de 2016 para dotar los créditos necesarios para la Fundación Teatro Romano de Cartagena, al objeto de abonar los intereses de demora generados por el vencimiento del Préstamo suscrito para la recuperación del Teatro Romano donde se ha transferido crédito entre partidas del mismo área de gasto, pero con diferente nivel de vinculación jurídica, recibiendo crédito la partida 2016.07001-3361-784, con documento contable de retención de crédito para transferir (RC2016.2.0026514.000), por importe de 26.000.-€ (veintiséis mil euros).

Dado que se hace necesario materializar el abono de los intereses de demora y atendiendo a la actividad de interés público que realiza la Fundación Teatro Romano de Cartagena, que no se ciñe sólo ni exclusivamente al término municipal, y siendo fundamental y necesario coadyuvar en sus gastos de funcionamiento (apertura, cierre, investigación, gestión y otros trabajos necesarios para la apertura del Teatro Romano de Cartagena y su Museo) así como inversiones a realizar para adecuar y recuperar espacios del Teatro Romano y su entorno y vistas las *Bases* de Ejecución del Presupuesto Municipal del Ayuntamiento de Cartagena y dado que la Fundación Teatro Romano cumple con los requisitos establecidos para

adquirir la condición de beneficiario de una subvención municipal.

En virtud de ello y de las competencias que han sido delegadas en la Junta de Gobierno Local según las Bases de Ejecución del Presupuesto General del año 2016, el Concejal del Área de Cultura, Patrimonio Arqueológico, Deportes y Juventud eleva propuesta a la Junta de Gobierno Local para que, si lo estima conveniente, acuerde:

1.- La aprobación del gasto de **26.000-€** (veintiséis mil euros) para transferir a la Fundación Teatro Romano de Cartagena, para lo que existe consignación presupuestaria por importe de **26.000- euros**.

2.- La aprobación de la concesión directa de la subvención por importe de **26.000.-€** (veintiséis mil euros) para transferir a la Fundación Teatro Romano de Cartagena, para lo que existe consignación presupuestaria por importe de 26.000 euros (veintiséis mil euros)

CONDICIONES

PRIMERA.- El pago de la presente subvención se realizará por el importe total de la misma mediante transferencia a la cuenta bancaria que designe el beneficiario en el acto expreso de aceptación de las condiciones a las que se somete el presente acuerdo de conformidad con lo dispuesto en las Bases de Ejecución del Presupuesto 2016.

SEGUNDA.- Son obligaciones del beneficiario las previstas en el artículo 14 de la Ley General de Subvenciones 38/2003 de 17 de noviembre y en las Bases de Ejecución del Presupuesto.

TERCERA.- Procederá el reintegro de la subvención en los términos establecidos en el artículo 37 de la Ley General de Subvenciones y en las Bases de Ejecución del Presupuesto por el procedimiento previsto en dichas Bases, así como por el incumplimiento de cualquiera de las Estipulaciones del presente acuerdo.

CUARTA.- El régimen jurídico al que se someten las partes en el presente procedimiento de subvención es el previsto en la Ley General de Subvenciones 38/2003 de 17 de noviembre, las Bases de Ejecución del Presupuesto Municipal , el RD 887/2006 de 21 de julio por el que se aprueba el Reglamento de la Ley General de Subvenciones, la Ley 7/1985 de 2 de abril y su normativa de desarrollo, el Decreto Legislativo 2/2004 de 5 de marzo por el que se aprueba el Texto Refundido de la Ley reguladora de Haciendas Locales, el presente acuerdo y en su defecto lo dispuesto en las Bases de Ejecución del Presupuesto 2016. En todo lo demás, se estará a lo dispuesto en el régimen jurídico aplicable al presente acuerdo.

El procedimiento aplicado es el de concesión directa, según lo dispuesto en las Bases de Ejecución del Presupuesto 2016 y el art: 22. 2 a) de la Ley General de Subvenciones 38/2003 de 17 de noviembre.

Cartagena a 27 de diciembre de 2016.= EL CONCEJAL DELEGADO DEL ÁREA DE CULTURA Y PATRIMONIO.= Firmado, Ricardo Segado García, rubricado.

La Junta de Gobierno Local acuerda aprobar, por unanimidad, al anterior propuesta.

DEPORTES

11. RECONOCIMIENTO EXTRAJUDICIAL DE CRÉDITOS DE FACTURAS CORRESPONDIENTES A LA LIMPIEZA DEL ESTADIO MUNICIPAL CARTAGONOVA, CON CARGO AL PRESUPUESTO MUNICIPAL VIGENTE.

Con fecha de julio de 2016 se aprobó el Convenio de colaboración entre la Concejalía de Deportes y el FC Cartagena sobre gestión y uso del Estadio Municipal Cartagonova donde se contempla en el apartado tercero punto decimocuarto que la obligación de limpieza corresponde al Ayuntamiento de Cartagena, cuya copia se adjunta.

Por parte de los Servicios Técnicos de Infraestructuras se está elaborando el Pliego de Prescripciones Técnicas para el nuevo contrato de limpieza del Estadio Municipal Cartagonova.

Dado que al día de la fecha aún no se ha contratado el servicio referenciado y en cumplimiento del informe realizado por la Interventora General Municipal de fecha 5 de agosto de 2016, es por lo que se procede a la tramitación del presente expediente extrajudicial de crédito para la tramitación y pago de las facturas generadas por el servicio mencionado durante los cinco meses de mayo, septiembre, octubre, noviembre y diciembre del presente año y que a continuación se relacionan.

PARTIDA PRESUPUESTARIA	IMPORTE	RFA. FRA.	TERCERO	NIF	DOCUMENTO DE CONSIGNACIÓN
07002.3420.2270000	5.639,81 €	2016.EMIT-64	GALMAR OBRAS Y SERVICIOS	B30844849	2016.2.0009585.000
07002.3420.2270000	7.095,44 €	2016.EMIT-2	GALMAR OBRAS Y SERVICIOS	B30844849	2016.2.0003971.000
07002.3420.2270000	6.521,90 €	2016.EMIT-7	GALMAR OBRAS Y SERVICIOS	B30844849	2016.2.0023534.000

07002.3420.2270000	5.353,04 €	2016.EMIT-8	GALMAR OBRAS Y SERVICIOS	B30844849	2016.2.0023535.000
07002.3420.2270000	3.143,58 €	2016.EMIT-10	GALMAR OBRAS Y SERVICIOS	B30844849	2016.2.0024442.000
TOTAL	27.753,77 €				

Por todo ello, solicito a la Junta de Gobierno Local, aprobar el reconocimiento extrajudicial de las facturas adjuntas que disponen de crédito presupuestario para su reconocimiento y liquidación, de las obligaciones derivadas de las facturas anteriormente relacionadas con cargo al Presupuesto Municipal vigente.

No obstante, la Junta de Gobierno Local, con su mejor criterio resolverá.= En Cartagena, a 19 de diciembre de 2016.= EL CONCEJAL DELEGADO DEL ÁREA DE CULTURA Y PATRIMONIO.= Firmado, Ricardo Segado García, rubricado.

La Junta de Gobierno Local acuerda aprobar, por unanimidad, al anterior propuesta.

12. SUBVENCIÓN POR CONCESIÓN DIRECTA A ENTIDADES DEPORTIVAS DE CARTAGENA.

El Excmo. Ayuntamiento de Cartagena de conformidad con el artículo 23 del Reglamento de Servicios de las Corporaciones Locales podrán conceder subvenciones a Entidades, Organismos o particulares, cuyos servicios o actividades complementen o suplan los atribuidos a la competencia local, en el artículo 2 de la Ley General de Subvenciones 38/2003 de 17 de noviembre, y en similares términos se manifiesta el artículo 44,2 c) de las Bases de Ejecución del Presupuesto de 2016, y conforme dispone también el artículo 17.2 de la Ley General de Subvenciones anteriormente mencionada.

Mediante Decreto de la Alcaldía-Presidencia de fecha 16-06-2015, se organizan las Áreas de Gobierno Municipales, creándose el Área de Cultura y Patrimonio, Juventud y Deportes. Dentro de sus programas de actuación, y como uno de los objetivos primordiales, está el potenciar el asociacionismo deportivo y la labor educativa que realizan los clubes de Cartagena en las tareas de promoción del deporte en el término municipal.

Así mismo, consta en el Presupuesto de Gastos del Área de Deportes, la partida asignada a Clubes, Asociaciones Deportivas, Centros Escolares y APAS en el capítulo de transferencias corrientes.
Se expresa en la Memoria justificativa el carácter singular de la subvención al Club deportivo PRIMISPORT y al Club deportivo Dolorense para el

desarrollo de la actividad deportiva del último trimestre del año 2016, en base al interés público y social de las actividades a subvencionar.

Este enorme esfuerzo deportivo-educativo que realizan los clubes y del que se benefician especialmente los jóvenes, conlleva numerosas dificultades de carácter económico, debido a que las entidades deben sufragar gastos de arbitrajes, desplazamientos, licencias federativas, equipamientos deportivos, etc., por ello se entiende que estas actividades de carácter social deben ser subvencionadas por el Ayuntamiento con la finalidad de contribuir a su eficacia y consolidación.

En virtud de ello, el Concejal del Área de Cultura y Patrimonio, Juventud y Deportes, eleva propuesta a la Junta de Gobierno Local, para que si así lo estima conveniente, acuerde:

1°. La aprobación del gasto de la subvención DE 2.000€ al Club Deportivo PRIMISPORT y de 8.000€ al Club Deportivo Dolorense, para sufragar las actividades correspondientes al último trimestre del ejercicio 2016 y estabilizar sus objetivos educativos y deportivos.

2°. Conceder subvención económica a los Clubes deportivos que a continuación se detallan, como financiación necesaria para finalizar las actividades del ejercicio 2016:

CLUB	CIF	CANTIDAD	PARTIDA
C. D. PRIMISPORT	G30773188	2.000€	2016.2.0026609.000
C. D. Dolorense	G30877609	8.000€	2016.2.0026610.000

El procedimiento previsto para la concesión de esta subvención es el de forma directa según lo dispuesto en los artículos 46 y siguientes de las Bases de Ejecución del Presupuesto y 22.2 c) de la Ley General de Subvenciones 38/2003 de 17 de noviembre. Consta en el expediente administrativo abierto al efecto, memoria justificativa del carácter singular de la subvención.

En Cartagena a 27 de diciembre de 2016.= EL CONCEJAL DELEGADO DEL ÁREA DE CULTURA Y PATRIMONIO.= Firmado, Ricardo Segado García, rubricado.

La Junta de Gobierno Local acuerda aprobar, por unanimidad, al anterior propuesta.

3°.- Informes de los Servicios y Negociados.

- **DACIÓN DE CUENTA DE RESOLUCIONES Y OTROS TÍTULOS HABILITANTES EN MATERIA DE INTERVENCIÓN URBANÍSTICA DICTADOS POR EL DIRECTOR GENERAL DE URBANISMO DESDE EL 14 AL 27 DE DICIEMBRE DE 2016 .**

Por el Sr. Alcalde, se dio cuenta a la Junta de Gobierno Local del Informe del Director General de Urbanismo relativo a las resoluciones y otros títulos habilitantes en materia de intervención urbanística tramitados desde el día 14 al 27 de diciembre de 2016, acompañando el siguiente documento resumen y quedando el listado anexo diligenciado:

A efectos de su conocimiento por la Junta de Gobierno Local, se adjunta relación de las **79 resoluciones adoptadas** en el Servicio de Intervención Urbanística de esta Dirección General de Urbanismo, durante el periodo comprendido **entre el 14/12/2016 y el 27/12/2016**, así como de los **57 títulos habilitantes** (Declaraciones responsables y Comunicaciones previas), presentados por los interesados, de conformidad con lo previsto en los arts. 264 y 265 de la Ley 13/2015, de 30 de marzo, de Ordenación Territorial y Urbanística de la Región de Murcia (BORM 06/04/2015).

Todo ello ha supuesto un **presupuesto** de ejecución de las actuaciones pretendidas **de 575.542,78€**, lo que supone un **ingreso en concepto de tasas de 23.015,08€, y consiguiente ingreso en concepto de ICIO de 23.021,71€.**

Destaca el **número de actuaciones** de construcción, adecuación, rehabilitación y reforma de viviendas **por un total de 5.**

Así como las actividades comerciales de ocio, restauración y servicios **con un total de 27**.

Cartagena a 28 de diciembre de 2016.= El Director General de Urbanismo.= Firmado, Jacinto Martínez Moncada, rubricado.

La Junta de Gobierno Local quedó enterada.

4º.- Manifestaciones del Excmo. Sr. Alcalde-Presidente.

No las hubo.

5º.- Ruegos y preguntas.

No se formularon.

Y no siendo otros los asuntos a tratar, la Presidencia levanta la sesión a las diez horas cinco minutos. Yo, Concejal Secretario, extiendo este Acta, que firmarán los llamados por la Ley a suscribirla. Doy fe.