Ámbito de la Administración Foral

# Sistema de protección de datos de carácter personal de la Cámara de Comptos de Navarra, ejercicios 2015-2016

Octubre de 2017

CÁMARA DE COMPTOS DE NAVARRA
NAFARROAKO KONTUEN GANBERA

www.camaradecomptos.org

# ÍNDICE

PÁGINA

## I. Introducción

La auditoría o fiscalización de cumplimiento de legalidad sobre el sistema de protección de datos de carácter personal de la Cámara de Comptos se realiza en cumplimiento de la Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos y del Documento de Seguridad de la propia Cámara, que establecen que los sistemas de información e instalaciones de tratamiento y almacenamiento de datos personales se someterán, al menos cada dos años, a una auditoría interna o externa.

La Cámara ha optado por la realización de auditorías o fiscalizaciones internas, siendo la última realizada la correspondiente a los ejercicios de 2012 y 2013, que se emitió en marzo de 2014.

Este trabajo, relativo a los ejercicios de 2015 y 2016, se ha incluido en el programa anual de fiscalización que la Cámara de Comptos para el año 2017 y lo ha realizado, en agosto de dicho año, un equipo integrado por una técnica de auditoría y un auditor, con la colaboración de los servicios jurídicos, informáticos y administrativos de la Cámara.

Al tratarse de un informe de auditoría o fiscalización interna, no se aplica el procedimiento de alegaciones previstos en el art. 11.2 de la Ley Foral 19/1984, reguladora de la Cámara de Comptos de Navarra.

Este informe será analizado por la responsable de seguridad que elevará las conclusiones a la responsable de los ficheros para que adopte las medidas necesarias y quedará a disposición de la Agencia Española de Protección de Datos.

## II. Protección de datos de carácter personal y normativa aplicable

### II.1. Aspectos generales

La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante, LOPDP) tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, el honor e intimidad personal y familiar. Se aplica a los datos de carácter personal registrados en soporte físico susceptibles de tratamiento y a toda modalidad de uso posterior de estos datos.

Se entiende por "dato personal" cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables. Una persona física no se considera identificable si su identificación requiere plazo o actividades desproporcionadas.

Se entiende por "tratamiento de datos" las operaciones y procedimientos técnicos que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo, cancelación y cesiones de datos.

Los datos de carácter personal se organizan en ficheros. La Cámara de Comptos, en el ejercicio de sus competencias, viene obligada al cumplimiento de la normativa reguladora de la protección de datos de carácter personal en aquellos ficheros automatizados y no automatizados de los que es responsable y que contengan datos de carácter personal.

La responsable de los ficheros es la presidenta de la Cámara de Comptos; asimismo se designó, de acuerdo con la normativa, una responsable de seguridad –una letrada– y un administrador de seguridad –un informático–. Cada fichero es responsabilidad de un encargado.

La normativa exige que se adopten las medidas de índole técnica y organizativas necesarias para garantizar la seguridad de los datos personales y evitar su alteración, pérdida, tratamiento o acceso no autorizado. Estas medidas de seguridad vendrán determinadas en función del carácter de los datos personales contenidos en los ficheros y se clasifican en tres niveles: alto, medio y bajo. Para cada uno de estos niveles se fijan las oportunas medidas de seguridad que corresponde adoptar.

Los ficheros de datos de carácter personal responsabilidad de la Cámara de Comptos de Navarra, su nivel de seguridad y los encargados de los mismos, se muestran en el siguiente cuadro:

| Ficheros | Nivel de seguridad | Encargado |
|---|---|---|
| Fichero de Registro General | Básico | Administrador |
| Fichero de Control de Accesos | Básico | Secretaria de la presidenta |
| Fichero de Gestión de Personal | Medio | Administrador |
| Fichero de Contabilidad y Gestión Económica Financiera | Medio | Administrador |
| Fichero de Fiscalización | Alto | Auditor responsable de la fiscalización o letrado responsable del asesoramiento |

El Documento de Seguridad de la Cámara de Comptos –aprobado inicialmente en diciembre de 2008 y modificado en septiembre de 2014– se aplica a los ficheros que contienen datos de carácter personal bajo la responsabilidad de la Cámara, incluyendo a los sistemas y equipos empleados para el tratamiento de dichos datos, a las personas que intervienen en el tratamiento y los locales en los que se ubican. La existencia de este Documento es un requisito de la normativa vigente y es de obligado cumplimiento por el personal de la Cámara con acceso a datos de carácter personal.

En el último informe de auditoría o fiscalización interna efectuado correspondiente a los ejercicios de 2012 y 2013, se concluía con la siguiente opinión:

*"En general, las medidas de seguridad y controles implantados en la Cámara de Comptos se adecuan a lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y en su Reglamento de Desarrollo aprobado por Real Decreto 1720/2007, de 21 de diciembre."*

## II.2. Normativa

La normativa reguladora de la materia objeto de revisión es básicamente la siguiente:

- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (texto consolidado de 5 de marzo de 2011)

- Real Decreto 1720/2007, de 21 de diciembre, del Reglamento de Desarrollo de la Ley Orgánica de Protección de datos de Carácter Personal (texto consolidado de 8 de marzo de 2012).

- Resolución del Presidente de la Cámara de Comptos de 22 de marzo de 2006, por la que se regula el fichero de "Registro General", el fichero de "Gestión de Personal" y el fichero de "Contabilidad y Gestión Económico-Financiera".

- Resolución del Presidente de la Cámara de Comptos, de 18 de diciembre de 2008, por la que se modifican los ficheros de "Gestión de Personal" y de "Contabilidad y Gestión Económico-financiera", y se aprueba la creación de dos nuevos ficheros: "Fichero de Control de Accesos" y "Fichero de Fiscalización".

- Resolución del Presidente de la Cámara de Comptos, de 23 de diciembre de 2008 por la que se aprueba el Documento de Seguridad de la Cámara de Comptos y se procede al nombramiento de la responsable de seguridad y del administrador de seguridad.

- Resolución del 16 de septiembre de 2014, del Presidente de la Cámara de Comptos por la que se aprueba la nueva versión del Documento de Seguridad de la Cámara de Comptos de Navarra.

Por otra parte, conviene indicar que el 25 de mayo de 2016 entró en vigor el Reglamento General de Protección de Datos Personales (RGPD) 2016/679 del Parlamento Europeo y del Consejo, que sustituirá a la actual normativa vigente y que comenzará a aplicarse efectivamente el 25 de mayo de 2018. Este periodo de dos años tiene como objetivo permitir que los Estados de la Unión Europea, las Instituciones y las empresas y organizaciones que tratan datos personales vayan preparándose y adaptándose para el momento en que el Reglamento sea aplicable.

## III. Opinión de cumplimiento de legalidad

Hemos fiscalizado el sistema de protección de datos de carácter personal aplicado por la Cámara de Comptos. El ámbito temporal de nuestra actuación se ha centrado en los ejercicios de 2015 y 2016.

La presidenta de la Cámara de Comptos es la responsable de los ficheros automatizados y no automatizados que contengan datos de carácter personal bajo la responsabilidad de la Cámara y de establecer los mecanismos de control interno que se consideren necesarios para la protección de tales datos.

Hemos llevado a cabo muestra actuación de conformidad con los principios fundamentales de fiscalización de las Instituciones Públicas de Control Externo. Dichos principios exigen que cumplamos los requerimientos de ética, así como que planifiquemos y ejecutemos la fiscalización con el fin de obtener una seguridad razonable de que el sistema de protección de datos de carácter personal aplicado por la Cámara de Comptos resulta en todos los aspectos significativos conforme con las normas reguladoras en esta materia.

Una fiscalización requiere la aplicación de procedimientos para obtener evidencia de auditoría sobre el cumplimiento de los aspectos relevantes establecidos en la normativa sobre protección de datos personales durante los ejercicios fiscalizados. Los procedimientos seleccionados dependen del juicio del auditor, incluida la valoración de los riesgos de incumplimientos significativos de la legalidad. Al efectuar dichas valoraciones del riesgo, el auditor tiene en cuenta el control interno relevante para garantizar el cumplimiento de la legalidad en materia de protección de datos personales, con el fin de diseñar los procedimientos de auditoría que sean adecuados en función de las circunstancias, y no con la finalidad de expresar una opinión sobre la eficacia del control interno de la entidad.

Consideramos que la evidencia de auditoría que hemos obtenido proporciona una base suficiente y adecuada para fundamentar nuestra opinión.

### *Opinión de cumplimiento de legalidad*

En nuestra opinión, el sistema de protección de datos de carácter personal implantado por la Cámara de Comptos resulta, en todos sus aspectos significativos, conforme a lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y en su reglamento de desarrollo.

## IV. Observaciones y comentarios que no afectan a la opinión. Recomendaciones

Como parte de la fiscalización realizada, a continuación se incluyen aquellas observaciones y comentarios que no afectan a la opinión emitida, junto con las recomendaciones que se considera precisas implantar para una mejora del sistema de protección de datos de carácter personal.

### IV.1. Seguimiento sobre el grado de aplicación de las recomendaciones que contenía el informe de los ejercicios 2012 y 2013

En relación con las recomendaciones que se reflejaban en el anterior informe de auditoría interna, concluimos que, en términos generales, se han aplicado las indicadas en dicho informe.

En concreto, merece destacarse la aprobación por el presidente de una versión actualizada del Documento de Seguridad de la Cámara de Comptos. Así, en septiembre de 2014, y a propuesta de la responsable de seguridad, se aprueba tal nueva versión que recoge, entre otras, las propuestas de mejora más relevantes que contenían los informes de auditoría interna anteriores; asimismo se incluyeron otras propuestas derivadas de la práctica del trabajo.

Al objeto de incrementar el grado de concienciación del personal de la Cámara sobre la protección de datos de carácter personal, consideramos conveniente:

*Difundir, entre el personal de la Cámara de Comptos y mediante las oportunas sesiones informativas, la nueva versión del Documento de Seguridad. Estas sesiones podrían servir igualmente para incidir en los aspectos prácticos en el uso, medidas y procedimientos de protección de datos de carácter personal en nuestros trabajos de fiscalización y en el resto de ficheros.*

### IV.2. Ficheros de datos de la Cámara de Comptos

Dentro de estos ficheros, el único que presenta un nivel alto de seguridad es el de fiscalización.

Con carácter previo recordamos que, de acuerdo con el art. 81.3. del Reglamento de la LOPDP, las medidas de seguridad de nivel alto se aplicarán a los siguientes ficheros o tratamiento de datos de carácter personal:

*a) Que se refieran a datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual.*
*b) Que contengan o se refieran a datos recabados para fines policiales sin consentimiento de las personas afectadas.*
*c) Que contengan datos derivados de actos de violencia de género.*

*En el caso de ficheros de la letra a), y de acuerdo con el art. 81.5. y 6. del Reglamento, bastará la aplicación de medidas de seguridad de nivel básico cuando:*

- *Los datos se utilicen con la única finalidad de realizar una transferencia dineraria a entidades de las que los afectados sean asociados o miembros;*
- *Se trate de ficheros o tratamientos no automatizados o sean tratamientos manuales de estos tipos de datos de forma incidental o accesoria, que no guarden relación con la finalidad del fichero.*
- *En los ficheros o tratamientos que contengan datos de salud, que se refieran exclusivamente al grado o condición de discapacidad o la simple declaración de invalidez, con motivo del cumplimiento de deberes públicos.*

Del trabajo realizado sobre el fichero de Fiscalización, destacamos:

• El encargado de cada fichero será el auditor/a o letrado/a responsable de la fiscalización o asesoramiento.

• El nivel de seguridad de cada trabajo se define por el auditor en la correspondiente memoria de planificación. Así en 2015, de 36 trabajos, 32 fueron catalogados como de nivel medio y 4 como de nivel básico; en 2016, de 30 trabajos, 28 fueron definidos como de nivel medio y dos como básico. Dentro de los anteriores trabajos, se incluyen los ayuntamientos cuya fiscalización está contratada con firmas externas.

• En cuanto al procedimiento de recogida de datos, se establece, como medidas de seguridad, que siempre que sea posible se solicitará y trabajará con datos disociados y además, que se procurará no trasladar, ni en sistemas automatizados ni en soporte papel, la documentación presentada que contenga datos de carácter personal. Se aceptan circunstancias excepcionales debidamente motivadas por escrito por el encargado del fichero.

• Se prevé la segregación del fichero principal de aquellos ficheros en los que, por la naturaleza de los datos que contengan o por su finalidad o uso, requieran la aplicación de un nivel de medidas de seguridad diferente al del sistema principal, siendo de aplicación para estos ficheros segregados las medidas de nivel alto previstas en el Documento de Seguridad.

En 2016, dentro del trabajo de Ayudas de emergencia social, se segregó un fichero de datos no automatizados, que se catalogó como de nivel alto; el Documento de Seguridad regula el procedimiento a seguir en tales situaciones, habiéndose verificado su adecuado cumplimiento y comprobado que, en TeamMate, el fichero automatizado relacionado con el anterior, no presenta datos personales que pudieran calificarse como de seguridad alta.

En las circularizaciones enviadas por la Cámara a proveedores, entidades financieras y asesores jurídicos, se hace mención expresa a que "*la solicitud está sujeta a lo previsto en la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal*".

Recomendamos,

• *Interiorizar, por el personal implicado en los procedimientos de fiscalización, la importancia de la protección de datos de carácter personal y las medidas de seguridad a adoptar en su caso. Posiblemente exigiría una nueva tarea de análisis, reflexión y divulgación a todo el personal de la Cámara sobre:*

*a) qué tipo de datos son personales o no personales, a efectos de la normativa vigente.*

*b) qué niveles de protección requieren los datos de carácter personal y sus consecuencias prácticas en los trabajos.*

*c) características que debe reunir la información para que no necesite protección.*

*d) segregación de ficheros, trámites y requisitos de los mismos.*

*e) archivo de los ficheros no informatizados de los trabajos de fiscalización.*

Sobre los trabajos encargados por la Cámara de Comptos a firmas privadas de auditoría para realizar la fiscalización de entidades locales efectuados en 2015, observamos que en los pliegos sí se hace mención a las obligaciones que a estos efectos prevé la LOPDP, pero en los contratos no se menciona expresamente. En las prórrogas de estos contratos para 2016 no se formalizó tal documento, aunque si hemos comprobado que en las cartas de aceptación por las empresas del encargo, se hace una referencia genérica al sometimiento a los pliegos.

En 2017, la contratación de estos trabajos se ha realizado directamente por razones de su importe, requiriendo solo reserva de crédito y presentación de factura. No se ha firmado el contrato oportuno, si bien en la resolución de presidencia se vincula genéricamente tal adjudicación a los pliegos del anterior proceso selectivo.

• *Documentar por escrito el tratamiento y finalidad a dar a los datos así como las medidas de seguridad a implantar por los terceros contratados por esta Cámara y comunicar tal situación a la responsable de seguridad.*

Del análisis efectuado sobre el resto de los ficheros de datos de la Cámara de Comptos, señalamos las siguientes recomendaciones:

• *Con carácter general, recordar a todos los usuarios la obligación de no revelar a terceros las claves de su acceso autorizado ni tenerlas a la vista.*

• *En el fichero de Control de Acceso, archivar las carpetas anteriores a 2015 en el archivo general dotado con llave.*

• *En el fichero de Gestión de Personal, salvo el programa de nóminas, el resto de ficheros automatizados se ubican en el servidor, unos en la carpeta de S/admin y, los relativos a intervención, en S/técnicos; en definitiva, se está po-*

*sibilitando el acceso a los mismos de personal no siempre autorizado. Estos ficheros solo deben ser accesible para el personal autorizado en el Documento de Seguridad y, en su caso, revisar si este Documento contempla suficientemente las personas con necesidades de acceso.*

• *Para el fichero de Contabilidad y Gestión Económico-Financiera, es aplicable lo comentado en la recomendación anterior sobre el acceso a los documentos informatizados de personal no incluido en el Documento de Seguridad.*

## IV.3. Medidas de seguridad

Los ficheros de datos de carácter personal responsabilidad de la Cámara de Comptos de Navarra y su nivel de seguridad se muestran en el siguiente cuadro:

| Ficheros | Nivel de seguridad |
|---|---|
| Fichero de Registro General | Básico |
| Fichero de Control de Accesos | Básico |
| Fichero de Gestión de Personal | Medio |
| Fichero de Contabilidad y Gestión Económica Financiera | Medio |
| Fichero de Fiscalización | Alto |

Todos los ficheros y tratamientos de datos de carácter personal deben adoptar, como mínimo, las medidas de seguridad de nivel básico. Estas medidas son las siguientes:

| Ficheros automatizados y no automatizados | Ficheros automatizados | Ficheros no automatizados |
|---|---|---|
| -Registro de Incidencias | -Identificación y autentificación | -Archivo |
| -Control de acceso | -Copias de respaldo y recuperación | -Dispositivos de almacenamiento |
| -Gestión de soportes | | -Custodia de soportes |

Además, al fichero de "Contabilidad y gestión económica financiera" y al fichero de "Gestión de personal" deben aplicarse medidas de seguridad de nivel medio. Finalmente, el fichero de Fiscalización, como ya se ha comentado, está calificado con un nivel de seguridad alto.

A continuación se analizan las medidas o aspectos de seguridad más relevantes implantadas en la Cámara de Comptos.

### *IV.3.1. Incidencias*

De acuerdo con la vigente normativa, se considera "incidencia de seguridad" cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos de carácter personal.

El vigente Documento de Seguridad de la Cámara regula en su epígrafe 6º "el procedimiento de notificación, gestión y respuesta ante las incidencias". Así se detalla que el usuario que la detecte, la comunicará por escrito y con un conjunto de información al Responsable de Seguridad y éste, por un lado, la anotará en el Registro de Incidencias y, por otro, deberá adoptarlas medidas oportunas para eliminar el daño causado por la incidencia o minorarlo.

En el periodo revisado no consta la existencia de incidencias en el correspondiente Registro.

### *IV.3.2. Control de acceso físico*

El Documento de Seguridad señala que exclusivamente el personal autorizado podrá tener acceso físico a los locales donde se encuentren ubicados los equipos que den soporte a los sistemas de información correspondientes a los ficheros determinados como de nivel medio o alto, y que la puerta estará equipada con un dispositivo de seguridad.

El personal autorizado para acceso físico de forma permanente es:

- Servicios informáticos de la Cámara
- Empresa de mantenimiento de comunicaciones
- Servicios de limpieza
- Servicios de seguridad

También está regulado el procedimiento de acceso físico para usuarios ocasionales.

Los locales donde se ubica el servidor de la Cámara están cerrados con una llave magnética que deja registro de las aperturas que ha habido. Cada usuario permanente tiene una llave con un identificador, de forma que queda constancia en el registro de qué llave se ha utilizado.

Para la lectura del registro, el administrador de seguridad, sin una periodicidad fija, debe descarga la información de la llave de la puerta con un aparato especial y lo vuelca en el ordenador.

*Recomendamos establecer una periodicidad fija para el análisis del registro de accesos de la llave magnética*

### *IV.3.3. Control de acceso a ficheros*

Las medidas de seguridad de nivel básico en relación con el control de acceso a ficheros automatizados y no automatizados son: existencia de una relación actualizada de usuarios y de accesos autorizados, control de acceso a cada usuario según las funciones asignadas, mecanismos para evitar el acceso a datos o recursos con derechos distintos de los autorizados, concesión de permisos de acceso solo por personal autorizado y mismas condiciones para personal ajeno con acceso a los recursos.

Para nivel medio y para ficheros automatizados, control de acceso físico a los locales donde se ubiquen los sistemas de información.

Para nivel alto y ficheros automatizados, registro de accesos con revisión mensual del mismo; para ficheros no automatizados, control de accesos autorizados e identificación de accesos para documentos accesibles por múltiples usuarios.

Para el control de accesos, está implantado el Registro de Identificación y Autorización de Acceso, gestionado por la Responsable de Seguridad y relacionándose los usuarios, perfiles de usuarios y accesos a los que están autorizados. También está regulado el procedimiento por escrito sobre altas, bajas y modificaciones de usuarios.

Del trabajo realizado, se desprenden las siguientes recomendaciones:

• *Debe aplicarse con rigor el procedimiento descrito en el Documento de Seguridad sobre comunicación de altas y bajas para el Registro o analizarse si el mismo se adecúa al funcionamiento normal de la Cámara.*

• *El Registro debe mantenerse actualizado de forma permanente en cuanto a altas y bajas de usuarios.*

Para los ficheros de nivel alto, el Documento de Seguridad regula un procedimiento de acceso específico así como la creación de un Registro Histórico (Log) de Acceso cuyo contenido se conservará al menos dos años. Este registro, competencia del Responsable de Seguridad, deberá revisarse una vez al mes.

Sin embargo, en la Cámara no hay un “Registro Histórico (Log)” de accesos a recursos informáticos, registro que si está previsto en el Documento de Seguridad.

Por otra parte, la realización de la mayor parte de los trabajos de fiscalización se ejecuta a través de la aplicación TeamMate. Para esta aplicación hay dos vías de acceso: para los trabajos en curso, cada equipo de auditoría tiene acceso a esa fiscalización con clave individualizada; para las fiscalizaciones finalizadas, en cambio, hay una clave común para todos los equipos de fiscalización. En el primer caso, queda registro en el sistema de los accesos realiza-

dos por los usuarios; en el segundo caso, sin embargo, no queda constancia del usuario particular que ha entrado en el sistema con la clave de consulta.

Recomendamos

• *Analizar la creación de un Registro Histórico (Log).*

• *Para proyectos catalogados como de seguridad alta y ya finalizados, adecuar la herramienta de TeamMate para controlar el acceso particular al proyecto de un usuario mediante la clave general.*

### *IV.3.4. Gestión de soportes y documentos*

Se considera soporte al objeto físico que almacena o contiene datos o documentos, o al objeto susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar y recuperar datos.

Todos los soportes y documentos con datos personales deberán estar identificados, etiquetados e inventariados.

• Identificación: Los soportes serán etiquetados para su identificación. La codificación se establecerá por el administrador de seguridad o, en su caso, por el encargado del fichero no automatizado.

• Etiquetado: En datos especialmente sensibles, el etiquetado será comprensible para los usuarios con acceso autorizado, dificultando la identificación para el resto.

• Inventario: Según el Documento de Seguridad, el inventario de soportes debe ser actualizado por el administrador de seguridad.

En el periodo revisado no ha sido necesario realizar ningún procedimiento de recuperación de datos de los ficheros automatizados que contuvieran datos de carácter personal

Del trabajo efectuado, destacamos las siguientes recomendaciones:

### *Inventario de soportes automatizados*

• *Inventariar los portátiles adquiridos después de 2012, especialmente si contienen o pueden contener datos de carácter personal. Igualmente actualizar su ubicación física.*

• *Actualizar el inventario de copias de seguridad con las realmente existentes y en los formatos que actualmente se pueden leer.*

• *Incluir los ordenadores de mesa en el inventario de soportes o establecer normas que limiten el mantenimiento de datos de carácter personal en los mismos.*

• *Incluir en el inventario de soportes las USBs especialmente si contiene datos de carácter personal.*

• *Para ordenadores portátiles y USBs, establecer normas concretas que desarrollen la obligación de borrar los datos de carácter personal que contienen los mismos, una vez que ya no se precisen o se termine el trabajo.*

### *Registro de entrada y salida de soportes*

• *Para ficheros de nivel medio, analizar si los soportes de datos personales utilizados en las fiscalizaciones deben anotarse en este registro de entrada.*

• *Para ficheros de nivel alto, reflejar en el registro el destino final de los soportes no automatizados utilizados: archivo, disociación o destrucción.*

### *Ficheros temporales*

*Tal como señala el Documento de Seguridad, todos los ficheros temporales y copias de trabajo que contengan datos de carácter personal deberán ser destruidos o borrados por el encargado del fichero o por persona por él autorizada, una vez que hayan dejado de ser necesarios para los objetivos por los que se crearon.*

### *Seguridad en trabajos fuera de la oficina*

*Todo el personal de fiscalización debe disponer y utilizar dispositivos USBs con contraseña cuando transporte información con datos de carácter personal.*

## *IV.3.5. Identificación y autentificación*

El mecanismo de autentificación e identificación de los usuarios a los ficheros automatizados que establece el documento de seguridad es el identificador de usuario y la contraseña. La política de contraseñas está regulada en la Instrucción 4/2007, de 20 de junio, del Presidente de la Cámara de Comptos, que establece la obligación de cambiarla semestralmente. Sin embargo y tal como la propia Instrucción refleja, esa periodicidad se ha acortado, en la actualidad, a un mes. Plazo este último que igualmente se refleja en el Documento de Seguridad.

## IV.4.Impacto del Reglamento General de Protección de Datos (RGPD) de la Unión Europea sobre la actividad de la Cámara de Comptos.

Este Reglamento empezará a aplicarse el 25 de mayo de 2018 y supone, esencialmente, la introducción –según la Agencia Española de Protección de Datos– de los siguientes cambios en las administraciones públicas sobre la actual regulación en materia de protección de datos personales:

• El Reglamento se basa esencialmente en medidas de prevención o responsabilidad activa. Es decir, las administraciones deben adoptar medidas que aseguren razonablemente que están en condiciones de cumplir con los principios, derechos y garantías que el Reglamento establece. Así, éste entiende que actuar solo cuando ya se ha producido una infracción es insuficiente como estrategia, dado que el posible daño causado al particular puede resultar difícil de reparar o compensar.

• Necesidad de efectuar un análisis de riesgo de todos los tratamientos de datos que se desarrollen por la administración y de revisar las medidas de seguridad que se apliquen en función de ese análisis de riesgo. Es decir, hasta ahora, las medidas de seguridad se fijaban atendiendo al tipo de datos; cuando entre en aplicación el Reglamento, las medidas de seguridad deben aplicarse atendiendo a las características de los tratamientos, sus riesgos, el contexto en que se desarrollan, la técnica y los costes.

• Necesidad de designar un Delegado de Protección de Datos que reúna cualidades profesionales y conocimientos de derecho y de práctica de la protección de datos personales. El Reglamento regula su posición en la organización y sus funciones, contemplando incluso la posibilidad de que los organismos públicos pueden nombrar un Delegado para varios de ellos, teniendo en cuenta su tamaño y estructura.

• Se establece el Registro de Actividades de Tratamiento, registro que sustituye, en parte, a la obligación de notificar los ficheros y tratamientos a las autoridades de protección de datos. Este Registro deberá mantenerse actualizado y a la disposición de las citadas autoridades.

• Necesidad de establecer mecanismos para identificar con rapidez la existencia de violaciones de seguridad de los datos personales y reaccionar ante ellas. Estas violaciones deberán ser notificadas a las autoridades de protección de datos y, si fuera necesario. a los interesados,

• Se introduce el derecho al olvido y el derecho a la portabilidad de los ciudadanos sobre los datos personales que se disponen por terceros.

*Recomendamos que se vayan dando los pasos precisos para adaptar las normas de protección de datos personales de la Cámara de Comptos a las exigencias que, en este ámbito, plantea el nuevo Reglamento Europeo. Resulta muy relevante el análisis de riesgo y la adopción de las medidas de seguridad derivadas del mismo así como el coste de su implantación y seguimiento; análisis que, en nuestra opinión, debería efectuarse mediante la constitución de grupos de trabajo con los implicados en la gestión de cada fichero.*

Pamplona, 10 de octubre de 2017

El auditor,

Ignacio Cabeza del Salvador