

Instrucción de Régimen Interior de la Secretaría General del Tribunal Constitucional, de 30 de julio de 2013, sobre medidas de seguridad de los ficheros del Tribunal Constitucional que contienen datos de carácter personal

Antecedentes:

- Instrucción de régimen interior de la Secretaría General de 20 de enero de 2000, por la que se establecen medidas de seguridad de los ficheros automatizados del Tribunal Constitucional que contienen datos de carácter personal
- Instrucción de régimen interior de 19 de febrero de 2007, de la Secretaría General, por la que se establecen medidas de seguridad de los ficheros automatizados del Tribunal Constitucional que contienen datos de carácter personal.
- Instrucción de régimen interior de la Secretaría General del Tribunal Constitucional, de 25 de enero de 2011, sobre medidas de seguridad de los ficheros del tribunal constitucional que contienen datos de carácter personal

Texto:

Las disposiciones de creación o modificación de un fichero deben indicar, entre otros aspectos, "*[l]as medidas de seguridad con indicación del nivel básico, medio o alto exigible*" [art. 20.2.h) de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (BOE núm. 298, de 14 de diciembre)]. A tal fin, el responsable del fichero o tratamiento deberá elaborar un "*Documento de seguridad*" que recogerá las medidas de índole técnica y organizativa, y será de obligado cumplimiento para el personal con acceso a los sistemas de información [art. 88 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 (BOE núm. 17, de 19 de enero de 2008)].

Al amparo de las previsiones de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (BOE núm. 262, de 31 de octubre), por Acuerdo del Pleno del Tribunal Constitucional de 16 de junio de 1994 (BOE núm. 155, de 30 de junio), se regularon los ficheros automatizados de datos de carácter personal existentes en el Tribunal Constitucional. No obstante, tras la aprobación de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y de su normativa de desarrollo, se dictó el Acuerdo del Pleno de Tribunal Constitucional de 21 de diciembre de 2006, por el que se regulan los ficheros automatizados de datos de carácter personal existentes en el Tribunal (BOE núm. 1, de 1 de enero de 2007), luego reformado, en lo atinente al número y — denominación de los ficheros automatizados de datos del Tribunal Constitucional, por el Acuerdo de 26 de marzo

de 2009 (BOE núm. 86, de 8 de abril), y, en lo referente al «Fichero de Usuarios de Sistemas de Información», por el Acuerdo de 28 de abril de 2010 (BOE núm. 105, de 30 de abril). De conformidad con ese Acuerdo "*[t]odos los ficheros del Tribunal Constitucional se encuentran sometidos a las medidas de seguridad de nivel medio que exige la legislación de protección de datos personales*" (art. 7).

Dado que la competencia para desarrollar y hacer cumplir los anteriores Acuerdos del Pleno corresponde a la Secretaría General del Tribunal Constitucional, bajo la autoridad de su Presidencia (art. 8.1 del Acuerdo de 21 de diciembre de 2006), tras una primera Instrucción de Régimen Interior de la Secretaría General del Tribunal Constitucional con fecha de 22 de marzo de 2000 por la que se establecían medidas de seguridad de los ficheros automatizados del Tribunal que contenían datos de carácter personal, se dictó posteriormente la Instrucción de 19 de febrero de 2007 por la que se establecían medidas de seguridad de los ficheros automatizados del Tribunal Constitucional (adaptándose al Acuerdo de 21 de diciembre de 2006), sustituida primero, por la Instrucción de 29 de abril de 2009 por la que se mantienen y adicionan medidas de seguridad de los ficheros automatizados del Tribunal que contienen datos de carácter personal (que se acomodaba al Acuerdo de 26 de marzo de 2009), y, luego, por la Instrucción de 25 de enero de 2011, sobre medidas de seguridad de los ficheros del Tribunal Constitucional que contienen datos de carácter personal (que se adaptaba al Acuerdo del Pleno de 28 de abril de 2010). Pues bien, si la auditoría relativa a las medidas de seguridad aplicadas en el tratamiento de datos de carácter personal de fecha 7 de diciembre de 2010 promovió que hubiera de dictarse una nueva Instrucción de Régimen Interior de la Secretaría General del Tribunal Constitucional, de 19 de julio de 2012, sobre medidas de seguridad de los ficheros del Tribunal Constitucional que contienen datos de carácter personal, que acogiera las modificaciones propuestas, la auditoría de 25 de noviembre de 2012 aconseja efectuar una doble adaptación: de un lado, para incorporar dentro de la Sección 1§ (Aspectos generales) un nuevo artículo sexto que regule el procedimiento para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición; de otro, para modificar la previsión de que la auditoría que verifique el cumplimiento de la legislación de protección de datos personales pueda ser no sólo externa sino también interna, tal como permite la normativa vigente.

Junto con los anteriores Acuerdos del Pleno del Tribunal Constitucional y las Instrucciones de Régimen Interior de la Secretaría General, se han venido adoptando por la Jefatura del Servicio de Informática, respecto del tratamiento automatizado de datos de carácter personal, un total de diez Directrices Técnicas de desarrollo [Acceso al sistema (DTS-01), Identificación y autenticación (DTS-02), Seguridad física y redes (DTS-03), Equipos y soportes (DTS-04), Internet, correo-e y comunicaciones (DTS-05), Pruebas (DTS-06), Copias de respaldo (DTS-07), Deberes del personal (DTS-08), Incidencias (DTS-09), Supervisión (DTS-10), y tres anejos [Ficheros de datos personales (DTS-AA), Recursos informáticos (DTS-AB) y Personal autorizado (DTS-AC)]. Y respecto del tratamiento no automatizado de datos de

carácter personal, otra Directriz Técnica de desarrollo [Protección de ficheros no automatizados (DTS-11)].

Pues bien, la experiencia y desarrollo en el Tribunal Constitucional de cuanto aparece afectado por la legislación de protección de datos de carácter personal, hacen necesaria la actualización de la citada Instrucción de Régimen Interior de la Secretaría General de 19 de julio de 2012. A tal fin, y puesto que las Instrucciones de Régimen Interior de la Secretaría General junto con las Directrices técnicas que la desarrollen constituyen, al amparo del art. 88 del Real Decreto 1720/2007, el *Documento de seguridad* que exige la normativa de protección de datos de carácter personal, en cumplimiento de lo dispuesto en el artículo 8.1 del Acuerdo del Pleno del Tribunal Constitucional de 21 de diciembre de 2006, por el que se regulan los ficheros automatizados de datos de carácter personal existentes en el Tribunal, previa conformidad de la Presidencia del Tribunal, en ejercicio de lo prevenido en el artículo 25.2 del Reglamento de Organización y Personal del Tribunal Constitucional, aprobado por Acuerdo del Pleno del Tribunal Constitucional de 5 de julio de 1990 [BOE núm. 185, de 3 de agosto], y de conformidad con apartado segundo del Acuerdo de 13 de abril de 2011, de la Secretaría General del Tribunal Constitucional (BOE núm. 90, de 15 de abril), que delega en el Secretario General Adjunto las competencias en materia de protección de datos de carácter personal, se dicta la presente Instrucción, con el contenido que se detalla a continuación.

Sección 1ª Aspectos generales

Artículo primero.- Ámbito de aplicación

1.- La presente Instrucción es de obligado cumplimiento para todos cuantos utilicen el sistema informático del Tribunal Constitucional y, de modo especial, para quienes cuenten con acceso autorizado a los ficheros automatizados de datos de carácter personal existentes en el propio Tribunal.

Será también aplicable, en lo que se acomode a su naturaleza y en los términos que se detallen en las Directrices Técnicas de Seguridad que la desarrollen, a los datos personales que sean objeto de tratamiento no automatizado.

2.- Será también aplicable, en lo que se acomode a su naturaleza y en los términos que se detallen en las Directrices Técnicas de Seguridad que la desarrollen, a los datos personales que sean objeto de tratamiento no automatizado.

3.- Las medidas de seguridad que se establecen se refieren a todos los componentes de los sistemas de información instalados en el Tribunal que contengan datos de carácter personal o que faciliten el acceso a los mismos, sin perjuicio de las garantías de carácter general establecidas por la legislación reguladora de esta materia.

4.- En todo caso, tanto los usuarios como la administración del sistema informático cumplirán con lo prevenido en el Acuerdo del Pleno del Tribunal Constitucional de 21 de diciembre de 2006 (modificado por el de 26 de marzo de 2009 y por el de

28 de abril de 2010), y, en lo que sea aplicable, 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.

Artículo segundo.- Documento de Seguridad

1. Integran el Documento de Seguridad la presente Instrucción y las Directrices Técnicas de Seguridad que la desarrollen, que serán aprobadas y actualizadas por el Servicio de Informática en lo que se refiere a los ficheros automatizados y, en lo atinente a los tratamientos no automatizados, por los Jefes de las Unidades y Servicios correspondientes.

2.- Los Servicios de Informática, Biblioteca, Doctrina Constitucional y Gerencia, en sus ámbitos respectivos, velarán por el cumplimiento del Documento de Seguridad y prestarán el asesoramiento y apoyo que a tal efecto se solicite por el resto de las Unidades y Servicios.

3.- Los Jefes de los distintos Servicios y Unidades harán cumplir en su ámbito propio lo dispuesto en el Documento de Seguridad y podrán proponer, a través del Letrado Jefe del Servicio de Informática o, en su caso, de la Gerencia, la adopción de medidas específicas para garantizar dicho cumplimiento.

4.- La presente Instrucción, junto con las Directrices Técnicas de Seguridad que la desarrollen, recogen las medidas de seguridad en materia de datos de carácter personal relativas a todos los ficheros y tratamientos de los sistemas de información del Tribunal Constitucional.

Artículo tercero.- Responsable de Seguridad

1.- El Responsable de Seguridad será único para todos los ficheros y tratamientos de datos de carácter personal.

2.- Corresponde al Responsable de Seguridad la coordinación y el control de las medidas establecidas por esta Instrucción y, en su desarrollo, por las Directrices Técnicas de Seguridad, para proteger los datos personales obrantes en los ficheros regulados por el Tribunal Constitucional.

3.- El Responsable de Seguridad será nombrado por la Presidencia del Tribunal Constitucional, a propuesta del Secretario General.

4.- Por Resolución de la Presidencia del Tribunal Constitucional de 21 de octubre de 2010 se acordó nombrar al Letrado al servicio del Tribunal Constitucional, don Herminio Losada González, como Responsable de Seguridad en materia de protección de datos de carácter personal.

Artículo cuarto.- Usuarios del sistema informático del Tribunal Constitucional

1. Tienen la condición de usuarios informáticos todas las personas que, por razón del ejercicio de sus funciones, están autorizadas a utilizar cualquiera de los recursos informáticos de la institución.

2.- También tendrán la consideración de usuarios informáticos aquellas personas que sean autorizadas a utilizar temporalmente los recursos informáticos de la institución.

3.- Son usuarios de los ficheros automatizados que contienen datos de carácter personal los usuarios a los que se refiere el núm. 1 de este artículo que estén expresamente autorizados para gestionar o consultar, en el cumplimiento de sus funciones propias, cualquiera de los ficheros regulados por el Tribunal Constitucional.

4.- No se permitirá el acceso de terceros a los datos personales albergados en los ficheros del Tribunal, salvo que sea necesario para la prestación de un servicio de tratamiento de datos en virtud del artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal o cuando sea preciso en cumplimiento de lo dispuesto en cualquier otro precepto de la citada Ley o de las disposiciones que la desarrollan o en otras normas con rango de ley.

5.- Para el caso previsto en el referido art. 12, en el expediente que se instruya al efecto se dejará constancia de la propuesta razonada del Jefe de la Unidad o Servicio competente, del informe del Servicio de Informática y del visado del Responsable de Seguridad. El Servicio de Informática asegurará el cumplimiento de las garantías previstas por la ley para estos accesos temporales.

Artículo quinto.- Identificación y autenticación de usuarios

1.- Cuando el mecanismo de acceso al sistema informático se base en contraseñas, los usuarios estarán identificados con un nombre y una contraseña personales que les permita el acceso al sistema.

2.- Cuando el mecanismo de acceso al sistema informático se base en tarjetas electrónicas, los usuarios contarán con una tarjeta individual y personalizada que les permita el acceso al sistema.

3. El acceso a determinados ficheros o recursos del sistema informático podrá quedar subordinado al uso de otras contraseñas adicionales.

4. La consulta de ficheros por usuarios ajenos a su gestión sólo procederá si las normas correspondientes del Documento de Seguridad así lo prevén específicamente y en los términos en que lo hagan.

Artículo sexto.- Derechos de acceso, rectificación, cancelación y oposición

1.- Las personas físicas titulares de los datos personales contenidos en los ficheros del Tribunal Constitucional podrán ejercitar, de forma gratuita, y personalmente o través de representante, en su caso, los derechos de acceso, rectificación, cancelación u oposición, ante la Secretaría General del Tribunal [calle Domenico Scarlatti, número 6 (28003-Madrid)].

2.- El derecho de acceso es el derecho a obtener información sobre si los datos de carácter personal están siendo objeto de tratamiento, la finalidad de dicho tratamiento, el origen de los datos y las comunicaciones realizadas o previstas de los mismos. El derecho de rectificación es derecho a modificar los datos inexactos o incompletos. El derecho de cancelación es el derecho a la supresión o bloqueo de los datos que resulten inadecuados o excesivos. Y el derecho de oposición es el derecho a que no se lleve a cabo el tratamiento de datos personales o a que se cese en el mismo, cuando exista un motivo legítimo y fundado que lo justifique.

3.- Para llevar a cabo el ejercicio de los derechos de acceso, rectificación, cancelación u oposición deberá dirigirse una comunicación a la Secretaría General del Tribunal Constitucional con el nombre y apellidos del interesado, petición en que se concreta la solicitud, dirección a efectos de notificaciones, fecha y firma. A tal comunicación se acompañará una fotocopia de su documento nacional de identidad (pasaporte u otro documento de identificación válido) y, en su caso, los documentos acreditativos de la petición formulada. Igualmente, en el supuesto de haberse conferido la representación, se acompañará a la anterior comunicación una fotocopia del documento nacional de identidad del representante (pasaporte u otro documento de identificación válido) y el documento acreditativo de la representación.

4.- La Secretaría General del Tribunal Constitucional resolverá en todo caso las peticiones relativas a los derechos de acceso, rectificación, cancelación y oposición. Dichas contestaciones deberán producirse, por escrito, en el caso del ejercicio del derecho de acceso, en el plazo máximo de un mes a contar desde la fecha de recepción de la solicitud, y en los supuestos del ejercicio de los derechos de rectificación, cancelación u oposición, en el plazo máximo de los 10 días hábiles siguientes al de recepción de la solicitud.

Sección 2ª Deberes de los usuarios

Artículo séptimo.- En general

1.- Todos los usuarios están obligados a respetar las normas de seguridad del sistema y a observar el secreto profesional.

2.- Los usuarios deben adoptar cuantas prevenciones sean precisas para garantizar la seguridad, la inalterabilidad y la confidencialidad de los datos de carácter personal a que tengan acceso por razón de sus funciones, incluso después de finalizar sus relaciones con el Tribunal Constitucional.

3. Los datos personales a los que se refiere esta Instrucción sólo serán utilizados para los fines expresamente previstos. Nadie, salvo el personal autorizado conforme a lo previsto en el artículo 4, apartados 4 y 5, de esta Instrucción, y en los términos establecidos en dichas normas, podrá llevar a cabo cualesquiera operaciones o actividades tendentes al conocimiento directo, copia o comunicación de los datos personales contenidos en los ficheros automatizados del Tribunal.

Artículo octavo.- Deberes relativos a las contraseñas y números de identificación personal (PIN)

- 1.- Los usuarios crearán y preservarán del conocimiento ajeno sus propias contraseñas o números de identificación personal (PIN).
- 2.- La contraseña o número de identificación personal se formará y, en su caso, se renovará, conforme a lo que dispongan las Directrices Técnicas de Seguridad.
- 3.- Antes de ausentarse del puesto de trabajo, los usuarios se asegurarán de que no se pueda acceder desde él a datos de carácter personal de los ficheros del Tribunal.

Artículo noveno.- Correo electrónico

- 1.- El correo electrónico del Tribunal dispondrá de las direcciones orgánicas que se precisen, a propuesta de los Jefes de los distintos Servicios y Unidades, así como de los buzones personales que se asignen a los usuarios.
- 2.- Los usuarios son responsables exclusivos del contenido de los mensajes que envíen a través del correo electrónico del Tribunal.

Artículo décimo.- Equipos

- 1.- Los usuarios velarán por la integridad y la conservación del equipamiento y de los accesorios puestos a su disposición por el Tribunal.
- 2.- La instalación en los equipos del Tribunal de programas o cualquier tipo de *software* no facilitados por el Tribunal Constitucional deberá ser comunicada con antelación a dicha administración.
- 3.- La conexión de equipos privados al sistema informático del Tribunal requerirá la previa autorización expresa de la administración del sistema.

Artículo undécimo.- Soportes

- 1.- Todos los soportes, tanto electrónicos como en papel, que contengan archivos o información del Tribunal con o sin datos de carácter personal, se custodiarán con el celo debido. Cada usuario es responsable de los soportes que le sean entregados por la administración del sistema.

- 2.- Los usuarios se abstendrán de realizar cualquier copia de ficheros que no venga estrictamente impuesta por el ejercicio de las funciones que tienen encomendadas.
- 3.- Los usuarios sólo pueden acceder a aquellos soportes con datos de carácter personal para los que estén autorizados. Los citados soportes deberán estar inventariados e identificar el tipo de la información que contienen.
- 4.- La salida fuera del Tribunal Constitucional de soportes que contengan datos de carácter personal, incluidos los comprendidos y/o anejos a un correo electrónico, salvo que se trate de datos que figuren en fuentes accesibles al público, deberá ser autorizada por la Secretaría General.
5. Cada usuario es responsable de los soportes que contengan datos de carácter personal, debiendo adoptar las medidas necesarias para evitar su sustracción, pérdida o el acceso indebido a la información que contienen.
6. Cuando vaya a desecharse un soporte que contenga datos de carácter personal deberá procederse a su destrucción o borrado, adoptándose las medidas necesarias para impedir el acceso a la información contenida en el mismo o su recuperación posterior.

Sección 3ª Los ficheros

Artículo duodécimo.- Normas generales

- 1.- En ningún caso se crearán otros ficheros con datos personales para cometidos del Tribunal Constitucional distintos de los que hayan sido regulados por el Tribunal Constitucional.
- 2.- Cuando los datos de carácter personal integrados en un fichero provengan de escritos o documentos remitidos al Tribunal Constitucional se registrarán previamente en el Registro General del Tribunal.

Artículo decimotercero.- El Fichero de Registro General

- 1.- *Finalidad:* Ordena la recepción de todos los escritos dirigidos al Tribunal y salida del mismo de los escritos y comunicaciones oficiales dirigidos a otros órganos o a particulares.
- 2.- *Servicio encargado del tratamiento:* Registro General, bajo la autoridad y supervisión del Secretario de Justicia encargado del mismo.
- 3.- *Gestión:* Sólo funcionarios del Registro General expresamente autorizados por el Secretario de Justicia del que depende el fichero.
- 4.- *Consulta:* mediante autorización expresa de la Secretaría General, cuando así resulte necesario para el desarrollo de las funciones respectivas.

Artículo decimocuarto.- El Fichero de Asuntos Jurisdiccionales

1.- *Finalidad:* Ordena los diferentes procesos de competencia de la jurisdicción constitucional ingresados en el Tribunal.

2.- *Servicios encargados del tratamiento:* Secretarías de Justicia en las que deben tramitarse los diferentes asuntos que hayan tenido entrada en el Tribunal Constitucional, bajo la autoridad y supervisión de los respectivos Secretarios de Justicia.

3.- *Gestión:* Sólo funcionarios del Registro General y de las Secretarías de Justicia expresamente autorizados, en cada caso, por los Secretarios de Justicia de quienes depende el fichero.

4.- *Consulta:* mediante autorización expresa de la Secretaría General, cuando así resulte necesario para el desarrollo de las funciones respectivas.

Artículo decimoquinto.- El Fichero auxiliar de Asuntos Jurisdiccionales

1.- *Finalidad:* Recoge los datos de quienes se dirigen al Tribunal Constitucional mediante escritos distintos a los que corresponde al Fichero de Asuntos Jurisdiccionales, así como la respuesta dada a los mismos por la autoridad correspondientes del Tribunal.

2.- *Servicio encargado del tratamiento:* Secretaría General y Gabinete Técnico de la Presidencia, en cada uno de sus propios ámbitos y bajo la autoridad y supervisión, respectivamente, del Secretario General y del Jefe del Gabinete Técnico.

2.- *Gestión:* Sólo personal de Secretaría General y del Gabinete Técnico expresamente autorizado, en cada caso, por el Secretario General o por el Jefe del Gabinete Técnico de la Presidencia.

Artículo decimosexto.- El Fichero de Personal

1.- *Finalidad:* Facilita la gestión administrativa y económica en todo lo relacionado con quienes prestan servicio en el Tribunal Constitucional.

2.- *Servicio encargado del tratamiento:* Gerencia del Tribunal, bajo la autoridad y supervisión del Gerente.

3.- *Gestión:* Sólo personal de Gerencia, expresamente autorizado por el Gerente. Ello sin perjuicio del acceso del personal al servicio del Tribunal a los datos de su propio expediente personal u otros de carácter personal obrantes en este fichero.

4.- *Consulta:* Jefatura de los distintos Servicios y Unidades en lo que interese, estrictamente, al cumplimiento de jornada y horario por el personal de su dependencia.

Artículo decimoséptimo.- El Fichero de Usuarios de Sistemas de Información

- 1.- *Finalidad:* Facilita la gestión del acceso a los sistemas de información y del control de las tarjetas y certificados electrónicos del Tribunal Constitucional.
- 2.- *Servicio encargado del tratamiento:* Servicio de Informática, bajo la autoridad y supervisión de su Letrado Jefe.
- 3.- *Gestión:* Sólo personal del Servicio de Informática expresamente autorizado por su Letrado Jefe.

Artículo decimooctavo.- El Fichero de Biblioteca

- 1.- *Finalidad:* Facilita la gestión del acceso a los libros y publicaciones periódicas de la Biblioteca.
- 2.- *Servicio encargado del tratamiento:* Biblioteca, bajo la autoridad y supervisión del Letrado Jefe del Servicio de Estudios, Biblioteca y Documentación.
- 3.- *Gestión:* Sólo personal de este servicio expresamente autorizado para ello por el Letrado Jefe del mismo.

Artículo decimonoveno.- El Fichero de Selección de Personal

- 1.- *Finalidad:* Facilita la gestión de los procedimientos administrativos para la selección de personal.
- 2.- *Servicio encargado del tratamiento:* Gerencia, bajo la autoridad y supervisión del Gerente.
- 3.- *Gestión:* Sólo personal de Gerencia expresamente autorizado por el Gerente. Asimismo, podrán tener acceso a este fichero, durante los procedimientos de selección de personal o de adjudicación de becas, los miembros de las respectivas comisiones de valoración.

Artículo vigésimo.- El Fichero de Control de Acceso

- 1.- *Finalidad:* garantiza la seguridad en el edificio sede del Tribunal Constitucional.
- 2.- *Servicio encargado del tratamiento:* Corresponde exclusivamente a la Comisaría Especial del Tribunal Constitucional, la gestión y consulta de este fichero, sin perjuicio de las funciones de coordinación administrativa que competen a la Gerencia del Tribunal, especialmente en cuanto al mantenimiento y aportación de los datos de todas las personas al servicio del Tribunal y a la gestión de las autorizaciones de utilización del garaje de su sede y dependencias. Todo ello en el marco de lo prevenido, con carácter general, en los apartados "a", "b" y "c" del art. 15 del Reglamento de Organización y Personal del Tribunal Constitucional.

3.- *Gestión*: Para la debida información a los interesados, se mantendrá bien visible en la puerta de acceso al edificio sede del Tribunal una advertencia en la que se especifique que el control de entrada al edificio está dotado, con fines de seguridad, de un registro fotográfico de los visitantes, y que tanto la fotografía obtenida como los datos personales que le acompañan se registran en un fichero automatizado del Tribunal durante el tiempo requerido por tales razones de seguridad, siendo cancelados, en todo caso, transcurrido un año desde su registro. Por último, se informará asimismo de que las solicitudes de acceso, rectificación y cancelación se dirigirán a la Secretaría General del Tribunal.

4.- Cuando los datos del Fichero de Control de Acceso hayan dejado de ser necesarios para la finalidad por la que se recabaron y, en todo caso, en el plazo de un año desde su obtención serán cancelados con las debidas garantías y mediante un procedimiento automatizado por la administración del sistema.

Sección 4ª La administración del sistema informático

Artículo vigésimo primero.- Seguridad física y redes

1.- Sólo podrá tener acceso a los locales donde se encuentran los servidores del sistema el personal expresamente autorizado por el Letrado Jefe del Servicio de Informática.

2.- El acceso remoto por los usuarios del sistema informático del Tribunal Constitucional a los que hace referencia el art. 4 de esta Instrucción a la red institucional propia requerirá de medidas de seguridad equiparables a las del acceso de forma local y, en todo caso, de la correspondiente habilitación expresa.

3.- Todos los equipos informáticos del Tribunal y, en particular, los dispositivos móviles, deben estar protegidos física y lógicamente.

Artículo vigésimo segundo.- Pruebas

Las pruebas para la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal se realizarán con las debidas garantías, conforme al procedimiento que se establezca en las Directrices Técnicas de Seguridad.

Artículo vigésimo tercero.- Copias de respaldo y recuperación

1.- Diariamente se realizarán copias de respaldo de los archivos que obran en los servidores del Centro de proceso de 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 al tiempo de producirse la pérdida o destrucción.

Artículo vigésimo cuarto.- Incidencias

1.- En el supuesto de detectarse alguna incidencia o anomalía que afecte o pueda afectar a la seguridad de los datos o del sistema informático, se pondrá en conocimiento inmediato tanto del Responsable de Seguridad como del Servicio de Informática, así como del Jefe de la Unidad o Servicio de quien dependa el fichero afectado.

2.- El personal no autorizado para acceder a los ficheros a que se refiere esta Instrucción pondrá en inmediato conocimiento del Responsable de Seguridad y del Jefe de la Unidad o Servicio a que esté asignado los datos a los que haya podido acceder por error o fallo de los sistemas de información.

Artículo vigésimo quinto.- Registro de incidencias

1.- El Servicio de Informática mantendrá ordenado y actualizado un registro de cualquier incidencia que afecte tanto a la seguridad de los datos como a la seguridad del sistema informático del Tribunal.

2.- En dicho registro deberá hacerse constar, al menos, el tipo de incidencia, el momento en que se ha producido o detectado, la persona que realiza la notificación, a quién se le comunica, los efectos que se hubieran derivado de la misma y las medidas correctoras aplicadas.

3.- También se hará constar en el registro los procedimientos realizados de recuperación de los datos, con indicación de la persona que ejecutó el proceso, los datos restaurados y, en su caso, los datos que hubiese sido necesario grabar manualmente en el proceso de recuperación.

Sección 5ª El acceso al sistema informático

Artículo vigésimo sexto.- Control de acceso

1.- Los usuarios sólo tendrán acceso a aquellos recursos que precisen para el desarrollo de sus funciones, debiendo contar con las correspondientes autorizaciones.

2.- Se adoptarán los mecanismos necesarios para garantizar la correcta identificación y autenticación de los usuarios, de forma inequívoca y personalizada. Igualmente, se adoptarán las medidas precisas para evitar que el acceso indebido de los usuarios a recursos con derechos distintos de los autorizados.

3.- La concesión, alteración o anulación de permisos para el acceso a los diferentes recursos corresponderá al Jefe de cada Unidad o Servicio de quienes dependan los ficheros que contengan datos de carácter personal, quienes comunicarán al Servicio de Informática, a través de su Letrado Jefe, la designación del personal de su dependencia autorizado para gestionar o consultar los respectivos ficheros, así como las restricciones establecidas.

4.- La Gerencia comunicará al Servicio de Informática, a través de su Letrado Jefe, la incorporación o cese de las personas que hayan de causar alta o baja como usuarios del sistema o, en su caso, como usuarios de uno o varios ficheros automatizados.

5.- El Servicio de Informática mantendrá actualizados los permisos de sistema correspondientes y las relaciones tanto de usuarios del sistema informático como de quienes tengan permisos de gestión o de mera consulta de los ficheros de datos. Tales relaciones deberán estar a disposición del Responsable de Seguridad y de la Secretaría General.

Artículo vigésimo séptimo.- Acceso con contraseñas

1.- Cuando el mecanismo de autenticación de los usuarios se base en contraseñas, el nombre y la contraseña inicial serán asignados por la administración del sistema informático con arreglo a pautas generales. Cada usuario determinará sus contraseñas. El procedimiento para la asignación, distribución y almacenamiento de las contraseñas garantizará su integridad y confidencialidad.

2.- El usuario no podrá ausentarse de su puesto de trabajo sin haber bloqueado su equipo de modo que no sea posible el acceso al sistema informático.

3.- Las contraseñas se almacenarán, durante su vigencia, de forma ininteligible.

Artículo vigésimo octavo.- Acceso con tarjetas electrónicas

1.- Cuando el mecanismo de autenticación de los usuarios se base en tarjetas de identificación electrónica con número de identificación personal se establecerá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad.

2.- Cada usuario es responsable de la custodia de su tarjeta electrónica, así como del número de identificación personal que la protege y del código de desbloqueo. El usuario no podrá ausentarse de su puesto de trabajo sin haber extraído la tarjeta electrónica de su equipo, dejándolo bloqueado de modo que no sea posible el acceso al sistema informático.

3.- Cuando vaya a desecharse una tarjeta de identificación electrónica deberá procederse a su destrucción.

Sección 6ª Tratamientos no automatizados de datos de carácter personal

Artículo vigésimo noveno.- Medidas de seguridad

1.- Los ficheros no automatizados deberán contar con las mismas medidas de seguridad, obligaciones y gestiones que los ficheros automatizados.

- 2.- Los espacios destinados al almacenamiento de los documentos con datos de carácter personal deben disponer de dispositivos de control de accesos y apertura.
- 3.- Sólo podrá tener acceso a los espacios en los que se custodia la documentación del Archivo General el personal del mismo así como el expresamente autorizado por el Archivero Jefe, de acuerdo con las normas que se aprueben al efecto.
- 4.- Los Jefes de las Unidades y Servicios de los que dependan los ficheros que contienen datos personales que, en parte, sean objeto de tratamiento no automatizado adoptarán las medidas necesarias para garantizar que únicamente tenga acceso a tales datos el personal autorizado para ello.
- 5.- Dichas medidas se trasladarán a la Secretaría General y se incorporarán al Documento de Seguridad a que se refiere el artículo segundo, en el que se integrarán, asimismo, las normas de Archivo General.
- 6.- Por la Gerencia se aprobará, a propuesta del Archivero Jefe, un plan de prevención y actuaciones en caso de siniestro en los depósitos del Archivo General del Tribunal Constitucional.

Sección 7ª Auditoría de seguridad

Artículo trigésimo.- Auditoría de seguridad

- 1.- Cada dos años, o antes si se producen modificaciones sustanciales en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas o, en todo caso, cuando así lo propusiere el Responsable de Seguridad, los sistemas de información e instalaciones de tratamiento de datos, así como los tratamientos no automatizados, serán sometidos a una auditoría interna o externa que verifique el cumplimiento de la legislación de protección de datos personales y de los procedimientos e instrucciones vigentes en materia de seguridad de datos.
- 2.- El Responsable de Seguridad analizará los informes de auditoría y elevará sus conclusiones a la Secretaría General, quien propondrá, cuando así proceda, la adopción de las medidas correctoras adecuadas.

DISPOSICIONES FINALES

- 1.- Se asegurará la difusión general, dentro del Tribunal, de la presente Instrucción. Sin perjuicio de ello, todo nuevo usuario recibirá una copia de la misma junto con la tarjeta de identificación electrónica que hace posible su acceso al sistema informático. Asimismo, se adoptarán las medidas necesarias para que todo el personal conozca las Directrices Técnicas de Seguridad y normas de seguridad que afecten al desarrollo de sus funciones, así como las responsabilidades que le corresponden en su cumplimiento.

2.- Queda sin efecto la Instrucción de Régimen Interior de la Secretaría General de 19 de julio de 2012, sobre medidas de seguridad de los ficheros del Tribunal Constitucional que contienen datos de carácter personal.