I. Comunidad Autónoma

3. Otras disposiciones

Consejería de Hacienda y Administración Pública
Agencia Tributaria de la Región de Murcia

1030 Orden de 30 de enero de 2017, de la Consejería de Hacienda y Administración Pública por la que se aprueba el manual de uso de medios electrónicos para el personal de la Administración Pública Regional.

En la actualidad la sociedad de la información ha irrumpido con fuerza en los sectores económicos y sociales, presentándose las nuevas tecnologías de la información y la comunicación como una nueva forma de servicio de gran valor que potencia y multiplica las posibilidades de servicio al ciudadano.

En la Administración Regional el avanzado estado y creciente uso de sistemas de información y dispositivos digitales, obliga la necesidad de establecer un marco de conducta o norma de uso adecuado de los sistemas de información que determine en qué condiciones deben emplearse los medios y recursos electrónicos, como instrumentos de trabajo para el desempeño de la actividad laboral, con el fin de garantizar la diligencia y eficiencia de las personas que prestan los servicios.

La Administración Regional, en su política de seguridad de la información, tiene como objetivo proteger la información y los servicios reduciendo los riesgos a los que están sometidos hasta un nivel que resulte aceptable, aplicando para ello el principio de proporcionalidad en el esfuerzo. Además velar por el uso correcto de los sistemas de información, así como desarrollar las buenas prácticas necesarias para la prevención, detección, respuesta y recuperación ante incidentes de seguridad.

Con ello se pretende lograr el alineamiento estratégico de la gestión de la seguridad de la información, la política de seguridad de la Administración Regional y las regulaciones establecidas 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, 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 el Decreto 302/2011, de 25 de noviembre, de Régimen Jurídico de la Gestión Electrónica de la Administración Pública de la Comunidad Autónoma de la Región de Murcia.

El Decreto 302/2011, de 25 de noviembre, de Régimen Jurídico de la Gestión Electrónica de la Administración Pública de la Comunidad Autónoma de la Región de Murcia, en su disposición adicional novena, señala que las consejerías competentes en materia de innovación de los servicios públicos y en materia de planificación informática y aplicaciones informáticas corporativas, aprobarán, mediante orden, un manual de uso de medios electrónicos para el personal de la Función Pública Regional. Es el Decreto de la Presidencia 18/2015, de 4 de julio, de reorganización de la Administración Regional, y sus sucesivas modificaciones, atribuye en su artículo 3 a la Consejería de Hacienda y Administración Pública, las competencias en estas materias.

En el año 2012, el Consejo de Gobierno aprobó un Código de Buenas Prácticas en el que se determinaba como fin último el crear en el entorno de la Administración Regional una cultura de racionalidad y ahorro en los recursos, por supuesto, uno de los elementos fundamentales para alcanzar este fin eran los distintos servicios de telecomunicaciones y tecnologías de la información.

El órgano responsable de las infraestructuras y aplicaciones informáticas también ha elaborado distintos documentos sobre el uso de las herramientas informáticas acompañándolos a los distintos manuales explicativos o documentos de preguntas más frecuentes (FAQ).

El uso inapropiado de los recursos tecnológicos expone a la Administración Pública Regional a riesgos de seguridad como ataques de virus, compromisos de los sistemas y servicios de red, o incumplimientos legales y, en todo caso, sobre-costes para el despliegue y mantenimiento de los servicios públicos, cuando no pérdida de información.

Todo el personal al servicio de la Administración Pública Regional debe ser consciente de la necesidad de garantizar la seguridad de los sistemas de información, así como que ellos mismos son una pieza esencial para el mantenimiento y mejora de la misma. El conocimiento de los riesgos es la primera línea de defensa para la seguridad de los sistemas de información. Es por ello que el personal al servicio de la Administración Pública Regional, incluido el personal docente no universitario, debe estar debidamente informado, concienciado y formado sobre esta materia para que pueda ser capaz de detectar posibles incidentes que pudieran perjudicar seriamente los sistemas de información.

Este manual detalla las conductas adecuadas a seguir por las personas empleadas públicas en el uso de los sistemas de información, establece al Centro de Atención a Usuarios (CAU) como el interlocutor operativo en materia de seguridad y buen uso de los sistemas de información, define el procedimiento para difundir los cambios en las normas de uso de los medios electrónicos que conforman los sistemas de información, se informa a las personas empleadas públicas de la capacidad de control por parte de la Administración, de los controles a realizar y de las funciones de los diferentes centros directivos en el mismo, las consecuencias de un mal uso y, por último, se asegura la adopción de medidas para una respuesta efectiva y proporcional ante incidentes de seguridad.

En su virtud, de conformidad con la disposición adicional novena del Decreto 302/2011, de 25 de noviembre, de Régimen Jurídico de la Gestión Electrónica de la Administración Pública de la Comunidad Autónoma de la Región de Murcia y con el artículo 3 del Decreto de la Presidencia 18/2015, de 4 de julio, de reorganización de la Administración Regional,

Dispongo:

Artículo 1.- Objeto.

Aprobar el Manual de uso de medios electrónicos para el personal de la Administración Pública Regional, cuyo texto se inserta como anexo.

Artículo 2.- Ámbito de aplicación.

Esta normativa de seguridad es de aplicación al personal empleado público de las Consejerías y Organismos Autónomos, así como al personal docente de enseñanza no universitaria.

Los restantes Entes que configuran el Sector Público Regional, deberán aprobar, en su caso, para el personal al servicio de los mismos, sus respectivos Manuales de uso de medios electrónicos, sin perjuicio de la aplicación subsidiaria del Manual que se recoge como anexo.

Disposición adicional única.- Pliegos de Cláusulas Administrativas Particulares.

En los documentos que rijan las contrataciones administrativas se deberán incluir aquellas cláusulas que, de conformidad con el Manual de comportamiento en el uso de medios electrónicos para el personal de la Administración Pública Regional, deban regir el comportamiento de los adjudicatarios y del personal a su servicio en la materia objeto del mencionado Manual.

Disposición final primera.- Actualización permanente.

El Manual de comportamiento en el uso de medios electrónicos para el personal de la Administración Pública Regional, se deberá mantener actualizado de forma permanente. Se desarrollará y perfeccionará a lo largo del tiempo en paralelo al progreso de los servicios de Administración electrónica, de la evolución tecnológica y de las nuevas amenazas que pudieran surgir.

Disposición final segunda.- Entrada en vigor.

La presente Orden entrará en vigor el día siguiente al de su publicación en el Boletín Oficial de la Región de Murcia.

Murcia, 30 de enero de 2017.—El Consejero de Hacienda y Administración Pública, Andrés Carrillo Sánchez.

Anexo

Manual de comportamiento en el uso de medios electrónicos para el personal de la Administración Pública Regional.

1. Objeto

Definir y establecer las pautas de comportamiento adecuado en el uso de los sistemas de información de la Administración Pública Regional y de los medios electrónicos que lo conforman y facilitan; en particular que las personas usuarias conozcan sus obligaciones y buenas prácticas en el cumplimiento de las medidas de seguridad a aplicar respecto a la información que manejan, teniendo en cuenta especialmente la legislación en materia de protección de datos de carácter personal y las medidas de seguridad establecidas por el Esquema Nacional de Seguridad.

2. Centros directivos

1. Los distintos centros directivos responsables de los sistemas de información serán los que:

a) Inicien, en su caso, las actuaciones tendentes a comprobar el uso realizado por los empleados públicos de los sistemas informáticos puestos a su disposición. Sin perjuicio de otras actividades, podrán solicitar a la Dirección General competente en materia informática, y esta le facilitará, la información que sobre dicho uso se almacene.

b) Velen por la adecuada definición de permisos en aplicaciones o herramientas informáticas para procesos o transacciones evitando aquellos innecesarios para la función encomendada al empleado público.

2. La Dirección General competente en materia informática:

a) Diseñará, construirá y operará los sistemas de información específicos para el almacenado de evidencias del uso del resto de sistemas de información, que requiera la normativa en materia de protección de datos de carácter personal, cumplimiento del Esquema Nacional de Seguridad, esta orden y la que resulte de su desarrollo.

b) Identificará y mantendrá inventariados los sistemas de información de uso autorizado y sus características, fijará, habilitará y ejecutará las medidas técnicas para garantizar el buen uso y protección de los sistemas de información, autorizar cambios en la configuración de dispositivos y medios de acceso, difundir el conocimiento de las normas de uso y, siguiendo las directrices de los centros directivos responsables de los sistemas de información, de expedir, suspender o revocar las credenciales y permisos para el acceso a los mismos.

c) Analizará la problemática que presenta el uso de los equipos y dispositivos no propios y, en su caso autorizará o denegará su uso, fijará y auditará las condiciones específicas de seguridad que deban cumplir, así como las condiciones específicas de su uso en lo relativo al acceso a sistemas de información.

d) En el caso de incidente de seguridad en los sistemas de información de la Administración Pública Regional procederá de oficio a las comprobaciones, configuraciones y aplicación de medidas necesarias en dispositivos y sistemas de información con la finalidad de detectar, investigar y resolver dicho incidente. Las comprobaciones serán proporcionadas en relación con la gravedad del incidente, recabando la información y evidencias necesarias a tal efecto. En caso necesario podrá revocar de forma preventiva, las credenciales de acceso a sistemas de información y/o retirar dispositivos hasta que se resuelva el incidente o se garantice el adecuado uso de estos.

e) Organizará el CAU y definirá los procedimientos y canales de comunicación que los usuarios deben emplear para gestión de incidentes, peticiones y consultas en relación relativas a la seguridad y uso de los distintos Sistemas de Información.

f) Comunicará a los centros directivos las distintas disposiciones, normas y recomendaciones en desarrollo y aplicación de esta orden que además comunicará a los usuarios mediante anuncios en el Tablón del Empleado. Información que mantendrá actualizada en la intranet; https://rica.carm.es/

3. Uso inadecuado de los sistemas de información

Se considera uso inadecuado de los sistemas de información, a aquella actuación de la persona usuaria no ajustada a los fines propios de su trabajo, o que pueda afectar a la seguridad de los sistemas de información de la Administración Pública Regional y de los datos que en ellos se encuentren, en cualquiera de sus dimensiones (disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad), independientemente de que el uso se produzca desde dentro o fuera de las dependencias de la Administración Pública Regional, o con equipos o dispositivos propios o ajenos a ella.

4. Normas de uso de aplicación general

La persona usuaria debe efectuar adecuado uso de los sistemas de información, con la lealtad y buena fe que deben guiar la actuación profesional de los empleados de la Administración Pública Regional y, en particular:

a) La persona usuaria no debe:

1.º Ocultar o falsificar la identidad en el proceso de creación de las credenciales de acceso a los sistemas de información.

2.º Tratar de evitar las medidas de protección de la información o explotar posibles fallos de seguridad de los sistemas de información.

3.º Destruir o alterar malintencionadamente los sistemas de información.

b) La persona usuaria debe:

1.º Emplear los sistemas de información únicamente para fines propios de su trabajo, siempre respetando la política, normativa y procedimientos de seguridad que le apliquen.

2.º Mantener en secreto y no divulgar por ningún medio, incluso después del fin de su relación con la Administración, la información confidencial a la que tenga acceso, salvo que la misma sea de carácter público o se encuentre autorizado para ello.

3.º Hacer un uso responsable y racional de los sistemas de información y no malgastar los recursos que los componen.

4.º Comunicar al CAU cualquier incidencia o evento sobre los que tenga conocimiento y que afecte o pueda afectar a la seguridad de los sistemas de información.

5.º Acceder únicamente a aquellos ficheros con datos de carácter personal para los que haya sido autorizado por el Responsable del fichero y actuar sobre los mismos solamente con el alcance y finalidad que le haya sido fijado.

6.º Respecto a las obligaciones de las personas usuarias en materia de secreto estadístico, se atenderá a las obligaciones referidas en el párrafo anterior y será de aplicación en cualquier caso, sean o no datos de carácter personal. Asimismo, y en el caso de usuarios designados para la realización de funciones de índole estadístico o de apoyo a las mismas, deberá atender adicionalmente a las normas que dicte el órgano regional en materia de Función Pública Estadística.

7.º Consultar periódicamente y conocer la información publicada en la intranet (rica.carm.es) sobre seguridad de los sistemas de información y sus normas de uso y atender las indicaciones del CAU en aspectos de seguridad y en particular ante un incidente de seguridad.

8.º Conocer y aplicar diligentemente el contenido de esta norma, sus disposiciones y normas de desarrollo.

c) Se recomienda:

Consultar al CAU cualquier duda sobre la seguridad y el uso de los sistemas de información.

5. Normas de uso de aplicación específica

1. De equipos y dispositivos

a) En relación con los equipos y dispositivos propios la persona usuaria no debe:

1.º Alterar, sin la debida autorización, cualquiera de los componentes físicos o lógicos de los equipos y dispositivos informáticos de la Administración Pública Regional.

2.º Instalar software sin autorización, en particular aplicaciones y programas no autorizadas y/o sin licencia.

3.º Incumplir con las condiciones de la licencia o de los derechos de autor.

4.º Conectar o modificar la red de comunicaciones corporativa mediante equipos y dispositivos sin autorización.

5.º Instalar o usar de forma malintencionada cualquier código malicioso que provoque el mal funcionamiento o sobrecarga de los equipos informáticos o redes de comunicaciones.

6.º Realizar de forma intencionada alguna actuación que interfiera en el funcionamiento normal de otros ordenadores, impresoras, dispositivos o redes, o que provoque la congestión de los enlaces de comunicaciones o sistemas informáticos.

7.º Monitorizar y rastrear las comunicaciones de los usuarios.

8.º Utilizar sin autorización herramientas de escaneo de redes o computadores, o buscadores de recursos compartidos.

9.º Acceder a equipos, dispositivos, ordenadores, servidores o aplicaciones a los que no estuviera autorizado.

10.º Almacenar información personal no relacionada con las funciones del puesto de trabajo.

b) la persona usuaria debe:

1.º Aplicar las directrices que sobre almacenamiento de información en el PC y almacenamiento en red, determine la Dirección General competente en materia informática.

2.º Apagar el equipo cada vez que concluya la jornada laboral o durante una ausencia prolongada.

3.º Bloquear el equipo en caso de ausentarse mediante la utilización de salvapantallas con contraseña o cualquier otro tipo de bloqueo.

4.º En el caso de las impresoras, faxes y dispositivos similares, debe asegurarse de que no quedan documentos que contengan datos confidenciales o personales a disposición de personal no autorizado.

5.º En caso de transportar soportes de información fuera de las dependencias administrativas aplicar las medidas necesarias para que no sean accesibles por personal no autorizado.

2. De aplicaciones informáticas y la información que contienen

En relación con las condiciones de seguridad en el uso de la información digital la persona usuaria no debe:

a) Depositar en la basura documentos legibles con información confidencial o personal.

b) Tratar o alterar el contenido de los sistemas de información por cualquier medio o programa sin autorización del Responsable del sistema de información. Cuando el sistema de información contenga datos de carácter personal además deberá disponer de la autorización del Responsable del Fichero en los términos recogidos por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

c) Acceder de forma intencionada y no autorizada a archivos que contengan información confidencial o reservada así como la disposición y manipulación de dicha información.

d) Alterar la información contenida en los sistemas de información y de los propios sistemas de información con carácter impropio, interesado y/o delictivo.

e) Instalar y utilizar aplicaciones informáticas, archivos, imágenes, documentos o programas que tengan un contenido ofensivo, pornográfico

o discriminatorio por razones de género, etnia, opción sexual, discapacidad o cualquier otra circunstancia personal o social.

f) La solicitud de asignación de permisos o perfiles en aplicaciones o herramientas informáticas para procesos o transacciones no necesarios para la función encomendada.

3. De portátiles y dispositivos móviles.

En relación con las condiciones de seguridad en el uso de portátiles y dispositivos móviles la persona usuaria debe:

a) Articular las medidas de protección oportunas para evitar que los portátiles y dispositivos móviles sean sustraídos.

b) Proteger la información confidencial almacenada en dispositivos y portátiles según las directrices de la Dirección General competente en materia informática.

c) Comunicar sin dilación al CAU la sustracción de estos equipos e informar del tipo de información contenida en ellos.

d) Las personas usuarias de estos equipos no cederán el mismo a terceras personas sin autorización.

4. Del correo electrónico

a) En relación con las condiciones de seguridad en el uso del correo electrónico la persona usuaria no debe:

1.º Responder a mensajes de correo en los que se pida cualquiera de sus credenciales, claves y contraseñas.

2.º Abrir mensajes de correo, o los ficheros adjuntos o enlaces que contenga cuando no provengan de fuentes de confianza.

3.º Utilizar la dirección de correo propia ni de otras personas usuarias de la Administración para fines no laborales.

4.º Darse de alta con su cuenta de correo corporativa en sitios web o servicios que no estén relacionados con la actividad laboral.

5.º Enviar mensajes de correo electrónico con contenido inadecuado, ilegal, ofensivo, difamatorio, inapropiado o discriminatorio por razón de sexo, raza, edad, discapacidad, que contengan programas informáticos sin licencia, que vulneren los derechos de propiedad intelectual de los mismos, de alerta de virus falsos o difusión de virus reales y código malicioso, o cualquier otro tipo de contenidos que puedan perjudicar a las personas usuarias, identidad e imagen corporativa y a los propios sistemas de información de la organización.

b) La persona usuaria debe:

Comunicar al CAU en caso de recepción de un mensaje presuntamente no confiable o sobre el que existen dudas de su autenticidad.

c) Se recomienda:

1.º Para la transmisión de información confidencial o especialmente sensibles, utilizar cifrado de los datos o emplear otros procedimientos de ocultamiento de la información.

2.º Enviar los mensajes de correo exclusivamente a las personas interesadas en el asunto del mismo, en especial cuando haya destinatarios fuera de la CARM. Emplear preferentemente para estos últimos casos el campo CCO (Con Copia Oculta) para las direcciones de la Administración Pública Regional.

3.º Indicar en el mensaje cuál es su contenido y el propósito de los ficheros adjuntos.

4.º Almacenar los documentos y archivos necesarios para el trabajo en carpetas de trabajo y borrarlos del buzón del correo.

5. Del antivirus

a) En relación con las condiciones de seguridad en el uso del antivirus la persona usuaria no debe:

1.º Desinstalar, desactivar total o parcialmente, ni desconfigurar el software de protección, ni tampoco detener sus tareas (análisis, actualización, etc.), ya sea temporal o permanentemente.

2.º Instalar otro tipo de software de protección no autorizado.

b) La persona usuaria debe:

Asegurarse de que el sistema antivirus está actualizado y operativo y notificar al CAU cualquier anomalía detectada.

6. Del acceso a Internet desde las dependencias de la Administración Pública Regional.

a) En relación con las condiciones de seguridad en el uso de Internet la persona usuaria no debe:

1.º Intentar usar dispositivos, aplicaciones, proxys u otros medios que eviten la aplicación de la norma de filtrado de contenidos o las medidas dispuestas al efecto por la APR.

2.º Realizar transferencia de información a Internet que no guarde relación con las funciones desempeñadas y tareas autorizadas.

3.º Remitir a internet o acceder a: contenido ilegal, ofensivo, racista, xenófobo o sexista, que no respete los derechos de propiedad intelectual, o que atente contra el honor y la intimidad de las personas o los derechos de los menores.

4.º Instalar un programa o ejecutar un archivo descargado de internet sin asegurarse de que el antivirus verifica la no existencia de código malicioso.

b) El usuario debe:

Comunicar al CAU si considera que alguna página de Internet no está autorizada y considera que debe estarlo.

c) Se recomienda:

Averiguar si una descarga se produce desde un "sitio" confiable.

No descargar archivos de Internet de sitios no confiables o no relacionados con el puesto de trabajo.

7. De las claves y sistemas de firma electrónica

a) En relación con las condiciones de seguridad en el uso de claves y sistemas de firma electrónica la persona usuaria no debe:

1.º Revelar o entregar las claves o sistemas de firma, bajo ningún concepto a otra persona, ni mantener las claves por escrito a la vista o al alcance de terceros.

2.º Introducir la contraseña utilizada para el acceso a los sistemas de información de la Administración Regional en aquellos sistemas que no sean propiedad de la Administración Pública Regional.

3.º Usar una cuenta de usuario para la que no se tiene autorización o credenciales.

b) La persona usuaria debe:

1.º Custodiar todo identificador, contraseña, certificado, tarjeta inteligente o demás sistemas de autenticación y firma electrónica empleados para el acceso a los sistemas de información de la información de la Administración Pública Regional, guardando la debida diligencia para impedir el acceso o conocimiento por otras personas.

2.º Comunicar al CAU la pérdida, olvido o sospecha de conocimiento por otra persona.

3.º Cambiar las contraseñas regularmente siguiendo las indicaciones del responsable del sistema de información y, al menos, se realizará una vez al año y siempre que haya cualquier indicación de posible compromiso en el sistema o en la contraseña.

4.º Utilizar contraseñas fuertes, cumpliendo con la política de contraseñas que establezca en cada momento la Dirección General competente mediante la parametrización del sistema de directorio corporativo.

6. Consecuencias del mal uso de los medios electrónicos

El mal uso de los medios electrónicos podrá conllevar consecuencias en los ámbitos, disciplinario, de responsabilidad civil y judicial, entre otros, de conformidad con la normativa reguladora de los mismos.

7. Glosario de términos

A los efectos de la presente norma, los términos empleados en este articulado tendrán el sentido que se establece en el Glosario de términos descrito a continuación y, en su defecto, en el anexo IV del 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 en el anexo 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.

a) Sistema de información: El conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir. Abarcando a todos los sistemas de información que prestan servicios a Consejerías y Organismos Autónomos, servidores y estaciones de trabajo, ordenadores de puesto de trabajo, equipos portátiles y tabletas electrónicas, teléfonos móviles, impresoras y otros periféricos y dispositivos de salida de datos, sistemas de localización, redes internas y externas, sistemas multiusuario y servicios de comunicaciones (transmisión telemática de voz, imagen, datos o documentos) y almacenamiento que sean de su propiedad o le presten servicio, así como las aplicaciones informáticas (software) que estén alojadas en cualquiera de los sistemas o infraestructuras referidos y de la información contenida en ellos.

b) Equipos y los dispositivos propios: Los recursos tecnológicos informáticos y de comunicaciones proporcionados por la Administración Pública Regional exclusivamente para el desempeño de las funciones encomendadas al personal.

c) La información digital: Los programas y datos incluidos en los sistemas de información de la Administración Pública Regional, así como su reproducción y almacenado en soportes físicos.

d) Persona usuaria: cualquier persona que ha interactuado, interactúa o interactuará con los sistemas de información de la Administración Pública Regional.

e) Contraseña fuerte: Características que posee una clave, que la hacen más difícil de adivinar tanto por humanos como por computadoras.

f) Datos de carácter personal: Cualquier información concerniente a personas físicas identificadas o identificables.

g) Información confidencial o sensible: Información que solo debe ser accesible por el personal autorizado. En general lo son los datos de carácter personal.

h) Phising: tipo de estafa cuyo objetivo es el de intentar obtener los datos personales, claves, cuentas bancarias, números de tarjeta de crédito, identidades, etc. de un usuario. Se basa en suplantar (copiar) la imagen de una empresa o entidad haciendo creer a la posible víctima que, realmente la solicitud de los datos procede del sitio "Oficial" cuando en realidad no lo es.

i) Soportes de información: Todo dispositivo capaz de albergar información. Ejemplo: Estaciones de trabajo, portátiles, discos duros externos, lápices de memoria…

j) Proxy: equipo intermediario situado entre el sistema de la persona usuaria e Internet.

k) Credenciales de acceso: Combinación del ID de la persona usuaria o ID de la cuenta más el (los) factor(es) utilizado(s) para autenticar a una persona, dispositivo o proceso.

l) Discos de red: dispositivos de almacenamiento a los que se accede desde los equipos personales a través de protocolos de red, que nos permiten compartir información.

m) Soporte físico: Objeto físico susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar o recuperar datos.

n) Responsable del fichero o del tratamiento: persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente. En el caso de entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados, se considerará responsable del tratamiento a la persona o personas integrantes de los mismos.