

III.- OTRAS DISPOSICIONES Y ACTOS

Consejería de Presidencia y Administraciones Públicas

Orden de 11/07/2012, de la Consejería de Presidencia y Administraciones Públicas y de la Consejería de Fomento, por la que se aprueba la instrucción sobre el uso aceptable de medios tecnológicos en la Administración de la Junta de Comunidades de Castilla-La Mancha. [2012/12185]

La Administración de la Junta de Comunidades de Castilla-La Mancha, en cumplimiento de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, y del Decreto 12/2010, de 16 de marzo, por el que se regula la utilización de medios electrónicos en la actividad de la Administración de la Junta de Comunidades de Castilla-La Mancha, está impulsando un ambicioso plan de introducción de la gestión electrónica en sus servicios y procedimientos, impulso que requiere garantizar la seguridad jurídica de todos los intervinientes en las relaciones electrónicas y la protección de la información administrativa.

La regulación de las pautas de comportamiento en la utilización de los medios tecnológicos de información y comunicación por los empleados públicos y por el personal externo que, eventualmente, acceda a medios electrónicos a través de las redes de la Administración regional, se ha de realizar bajo dos premisas:

1. La eficacia, eficiencia y economía que debe presidir el funcionamiento de la Administración Pública y que exige un uso adecuado y controlado de los recursos, siguiendo las directrices que se recoge en el Plan de Garantías de los Servicios Sociales Básicos.
2. El respeto a los derechos constitucionales a la intimidad y la inviolabilidad de las comunicaciones.

Junto a los ordenadores personales, portátiles, faxes, impresoras o teléfonos, es importante destacar que existen otros recursos, como el ancho de banda, que son limitados y costosos, cuya utilización abusiva y descontrolada podría interferir en el desempeño de tareas necesarias y comprometer la calidad en el servicio público prestado a los ciudadanos.

El Decreto 14/2012, de 26 de enero, por el que se establece la estructura orgánica y se fijan las competencias de los órganos integrados en la Presidencia de la Junta de Comunidades de Castilla-La Mancha, en su artículo 10.1, asigna a la Dirección General de la Función Pública y Justicia la elaboración, gestión y coordinación de proyectos para la adecuación de la Administración regional a la normativa vigente en materia de seguridad y protección de datos de carácter personal. Asimismo el Decreto 125/2011, de 7 de julio, por el que se establece la estructura orgánica y las competencias de los distintos órganos de la Consejería de Fomento, en su artículo 11.2, asigna a la Dirección General de Telecomunicaciones y Nuevas Tecnologías la dirección, coordinación y seguimiento de las actuaciones en infraestructuras de tecnologías de la información y comunicaciones.

Por ello, la integración entre la seguridad jurídica de los intervinientes en las relaciones electrónicas y el uso aceptable de los medios electrónicos ha motivado la elaboración de esta orden conjunta, que aprueba la instrucción sobre el uso aceptable de medios tecnológicos en la Administración de la Junta de Comunidades de Castilla-La Mancha que ha sido acordada por la Comisión de Administración Electrónica y Simplificación de Trámites Administrativos.

En su virtud, disponemos

Artículo único. Aprobación de la instrucción.

Se aprueba la instrucción sobre el uso aceptable de medios tecnológicos en la Administración de la Junta de Comunidades de Castilla-La Mancha, que se inserta como anexo, la cual será de obligado cumplimiento por el personal de la Administración de la Junta de Comunidades y por el personal externo que utilice los medios electrónicos de la dicha Administración, desde la publicación de la presente disposición en el Diario Oficial de Castilla-La Mancha.

Disposición final única. Entrada en vigor.

La presente Orden entrará en vigor el mismo día de su publicación en el Diario Oficial de Castilla-La Mancha y se publicará también en la sede electrónica de la Administración de la Junta de Comunidades de Castilla-La Mancha, www.jccm.es.

Toledo, 11 de julio de 2012

El Consejero de Presidencia y Administraciones Públicas
LEANDRO ESTEBAN VILLAMOR

La Consejera de Fomento
MARTA GARCÍA DE LA CALZADA

Anexo

Instrucción sobre el uso aceptable de medios tecnológicos en la Administración de la Junta de Comunidades de Castilla-La Mancha

Capítulo I
Introducción

Primero. Objeto y ámbito de aplicación.

La presente instrucción tiene por objeto regular la utilización de los recursos tecnológicos que forman parte de los sistemas de información y redes de comunicación de la Administración de la Junta de Comunidades de Castilla-La Mancha y de las entidades de Derecho Público con personalidad jurídica propia, vinculadas o dependientes de la misma, por parte de su personal para el desempeño de sus funciones, así como del personal externo que presta sus servicios en las dependencias administrativas o que eventualmente acceda a ellos.

Segundo. Propiedad y uso de la información.

1. El derecho de uso de toda la información contenida en los equipos informáticos, correo electrónico, dispositivos de almacenamiento, servidores o que circule por su red corporativa es de la Administración. La propiedad de dicha información será de la Administración, sin perjuicio de la aplicación de lo previsto en la legislación vigente sobre propiedad intelectual.

2. No está permitida la utilización de la información para cualquier finalidad no prevista por la Administración, asumiendo los usuarios las siguientes obligaciones:

- a) Abstenerse de efectuar cualquier tratamiento con los datos suministrados por la Administración o recibidos de terceros, para finalidades distintas del cumplimiento de la función encomendada a su puesto de trabajo.
- b) Proteger la información, evitando el envío no autorizado de la misma al exterior, incluyendo la visualización de la misma. Esta protección incluirá la no revelación de información confidencial a través del teléfono o mediante mensajes en contestadores telefónicos o sistemas de mensajería vocal.
- c) Las empresas externas, proveedores o terceros que presten servicios informáticos y que tengan acceso a información de la Administración no podrán ceder dichos datos o archivos a terceros no autorizados.

3. La información contenida en el disco duro de los ordenadores personal de los empleados públicos es responsabilidad directa de estos. El personal técnico no podrá tener capacidad de acceso a los mismos salvo para los fines establecidos en el apartado decimoquinto, 3, de la presente instrucción, previa autorización expresa de la Secretaría General correspondiente o de la Dirección General competente en materia de tecnologías de la información y con notificación expresa al interesado.

Capítulo II
Medios tecnológicos

Tercero. Propiedad de los medios tecnológicos.

1. Todos los equipos informáticos, ordenadores personales y portátiles, así como impresoras, fotocopadoras, teléfonos y demás dispositivos físicos del entorno informático y de comunicaciones, adquiridos o suministrados por

la Administración son de su propiedad y proporcionará a cada usuario los medios tecnológicos necesarios para el desarrollo de sus funciones laborales, responsabilizándose el usuario de su correcta utilización.

2. La Administración podrá aplicar en los ordenadores personales y redes corporativas mecanismos automatizados de seguridad.

Cuarto. Puesto de trabajo seguro y política de escritorio limpio.

1. Todo usuario dispondrá de un usuario y una contraseña, que serán personales e intransferibles, con los que se realizará el inicio de sesión y el acceso a los sistemas de información a los que esté autorizado.

2. Las labores de instalación, mantenimiento, reparación, configuración del sistema operativo, manipulación de los mecanismos de seguridad o traslado, se realizarán por el personal autorizado a tal fin, debiendo los usuarios respetar la integridad de los equipos, sin ocasionar daños físicos o lógicos por un uso negligente de los mismos.

3. Responsabilidades de uso:

a) Las credenciales se guardarán con la máxima diligencia y confidencialidad, siendo el usuario responsable de su buen uso. Si un usuario tiene sospechas de que su contraseña está siendo utilizada por otra persona, deberá proceder a su cambio y contactar con el área indicada para notificar la incidencia.

b) La instalación de las aplicaciones informáticas necesarias para el desarrollo de las funciones del usuario deberá solicitarse a la unidad que preste servicios informáticos en la Consejería u organismo al que pertenezca.

c) El acceso a los sistemas informáticos tendrá la finalidad exclusiva de cumplir con las funciones autorizadas.

d) Como regla general, para el almacenamiento de información que deba ser compartida entre varios usuarios, y especialmente para datos de carácter personal, se utilizarán recursos de red con restricciones de acceso a usuarios autorizados.

e) Los usuarios deberán velar para que los equipos queden protegidos cuando vayan a quedar desatendidos; los puestos de trabajo estarán configurados de modo que, después de cinco minutos de inactividad, el sistema se bloquee automáticamente y el usuario tenga que proporcionar su contraseña de acceso para poder operar de nuevo. Además, se activará el bloqueo de pantalla con contraseña en los ordenadores cuando se deje el equipo desatendido. Cuando se termine la jornada de trabajo se deberá desconectar todos los dispositivos y terminales que no vayan a ser utilizados.

f) Los documentos y soportes que contengan información sensible o confidencial permanecerán guardados bajo llave cuando no se estén utilizando, especialmente si el usuario no se encuentra en su puesto de trabajo o la oficina está vacía.

Quinto. Equipos portátiles.

1. Los equipos portátiles se considerarán y tratarán como los equipos de sobremesa. Deberán configurarse de modo que se requiera una contraseña antes de producirse el arranque del sistema.

2. Responsabilidades de uso:

a) Se recomienda no almacenar información sensible o confidencial en este tipo de equipos, en caso de ser necesario deberá ser protegida mediante herramientas de cifrado.

b) No se dejará el portátil desatendido o abandonado en lugares donde pueda ser sustraído con facilidad. La pérdida o robo de cualquier dispositivo o equipo portátil deberá notificarse de inmediato al responsable correspondiente.

Sexto. Dispositivos móviles.

Las responsabilidades de uso son las siguientes:

a) Se debe evitar perder de vista el dispositivo y, en caso de pérdida o robo, informar lo antes posible para proceder a su bloqueo.

b) Los dispositivos deberán tener activado el bloqueo por PIN y, siempre que lo permitan, se activará la opción de bloqueo de terminal cada cierto tiempo y la solicitud de una contraseña para desbloquearlo.

c) No se permite el uso del dispositivo móvil con SIM ajenas a la Administración ni la modificación del hardware o software del dispositivo móvil sin previa autorización.

- d) Siempre que sea posible, no se almacenará la información sensible en los dispositivos móviles, asegurándose de limpiar los archivos temporales periódicamente.
- e) Se podrán utilizar programas de cifrado para proteger la información sensible.
- f) Solo se realizarán conexiones de dispositivos móviles a redes inalámbricas que ofrezcan confianza.
- g) El bluetooth se desconectará siempre que no se utilice. Estará configurado como oculto y con contraseña. No se permite la conexión a un dispositivo bluetooth de origen desconocido y se evitará realizar emparejamientos en lugares públicos.
- h) El usuario será responsable de realizar las copias de respaldo de la información almacenada en el dispositivo móvil.

Séptimo. Impresoras, fotocopiadoras, escáneres y fax.

1. Estos dispositivos se utilizarán cuando exista una necesidad real siendo responsabilidad del usuario la reproducción o envío de la información.
2. Se retirará sin retraso injustificado la información de los dispositivos y especialmente cuando contenga datos de carácter personal, sensible o confidencial.
3. Con carácter general, la realización de impresiones se realizará a doble cara, en blanco y negro, en papel reciclado y evitando realizar copias de documentación sensible.
4. Con carácter general, se sustituirán los faxes tradicionales por el sistema corporativo de fax-IP basado en correo electrónico que permite un aumento de la seguridad y una disminución de costes operativos.

Octavo. Telefonía fija.

1. Con carácter general, el personal al servicio de la Administración dispondrá de una línea de telefonía fija siempre que el desempeño de las funciones encomendadas lo requiera.
2. Se activarán sistemas de control de las líneas fijas colectivas que no tienen adscripción individualizada, de modo que se garantice un uso adecuado.
3. Las líneas de telefonía fija se ajustarán a las necesidades de cada usuario y los servicios se contratarán en función de perfiles de uso y necesidades de tráfico.
4. Las comunicaciones necesarias que deban ser realizadas a través de llamadas que no permita el perfil del usuario, se efectuarán a través de las secretarías de los órganos donde se encuentre adscrito el usuario.
5. Los servicios de llamadas internacionales tan sólo estarán disponibles, de manera restringida, en aquellas líneas que se autoricen expresamente por los titulares de las Secretarías Generales.

Noveno. Telefonía móvil.

1. El personal al servicio de la Administración dispondrá de este tipo de recursos cuando la naturaleza de las funciones encomendadas lo justifique y previa autorización del titular de la Secretaría General de la Consejería u órgano equivalente en el resto de organismos dependientes.
2. Justificada la necesidad de disponer de teléfono móvil, se clasificará a los usuarios según perfiles de uso.
3. Existe un perfil de datos para aquellos usuarios que deban utilizar acceso a datos de Internet, que en todo caso tendrá habilitada tarifa plana.
4. El servicio de datos internacional se encontrará desactivado; podrá ser autorizado puntualmente en casos debidamente motivados o bien se puede autorizar la utilización de bonos con importe limitado para su consumo en el extranjero.
5. Salvo casos plenamente justificados, todas las líneas de telefonía móvil dadas de alta en el servicio corporativo tendrán establecido un aviso de consumo mensual, referente al coste de la línea, de cómputo mensual y en función del perfil al que se encuentren adscritas.

6. Los titulares de las Secretarías Generales u órgano equivalente en el resto de organismos dependientes adoptarán las decisiones que correspondan para el supuesto de eventos excepcionales. Asimismo, velarán por el uso racional y eficiente de los medios de comunicación asignados al personal de sus respectivos departamentos, pudiendo exigir en cualquier momento, al objeto de verificar que responden a las necesidades del servicio, información detallada sobre el desglose de llamadas efectuadas.

Décimo. Acceso a internet.

1. Internet es una herramienta de trabajo puesta a disposición de los usuarios para ayudar en el desempeño de sus funciones. El acceso se realizará únicamente a través de la red establecida a estos efectos por la Dirección General competente en materia de infraestructuras y servicios comunes de tecnologías de la información y comunicaciones y a través de los medios tecnológicos que la Administración pone a disposición para tal fin. En caso de que, por necesidades de servicio, se requiriera la instalación de un proxy deberá solicitarse a dicha Dirección General, quien, en caso de aprobación, será la encargada de su instalación.

2. Con carácter general todas las estaciones de trabajo de la red corporativa tendrán acceso al servidor institucional www.jccm.es y a toda la Intranet.

3. Reglas de acceso:

a) Los recursos estarán clasificados según su contenido a través de sistemas automatizados y cada usuario tendrá asignado un perfil de acceso en función de su puesto de trabajo, que determinará a qué tipo de contenidos podrá acceder y en qué horarios.

b) Los perfiles de acceso serán creados por la Dirección General competente en materia de infraestructuras y servicios comunes de tecnologías de la información y comunicaciones, correspondiendo a las Secretarías Generales la autorización del acceso de los distintos puestos de trabajo, el establecimiento y asignación de los diferentes perfiles de restricción de contenidos a los que se podrá acceder en función de las necesidades del servicio que corresponda y la elección del mecanismo de control de accesos facilitando a la persona un usuario y una contraseña.

c) Cualquier usuario podrá solicitar la revisión de sus datos de conexión y navegación mediante petición dirigida a la Dirección General competente en materia de infraestructuras y servicios comunes de tecnologías de la información y comunicaciones, solicitud tramitada a través de la Secretaría General correspondiente.

d) La Administración podrá restringir el acceso a determinadas páginas web que por su contenido se consideren innecesarias para la organización o inseguras.

4. Responsabilidades de uso:

a) El acceso a Internet deberá ser responsable y racional, dentro del marco de la legalidad y sin atentar, en ningún caso, contra los derechos fundamentales de las personas.

b) Cada usuario será responsable de salvaguardar sus datos de autenticación y del uso de Internet que se haga a través de los mismos.

c) El hecho de que la Administración no haya bloqueado el acceso a una determinada página web no implica que el acceso a la misma sea autorizado.

d) No está permitido el acceso a páginas web de contenido ofensivo, inapropiado, pornográfico, erótico o discriminatorio por razones de género, etnia, opción sexual, discapacidad o cualquier otra circunstancia personal o social.

e) No se permite la descarga desde Internet de cualquier clase de programas, aplicaciones, documentos o archivos que no provengan de páginas oficiales y/o relacionadas con el trabajo, todo ello con la finalidad de que la descarga no pueda poner en peligro el sistema informático de la Administración.

f) No está permitida la utilización de la conexión a Internet para el desempeño de cualquier actividad profesional, por cuenta propia o ajena, distinta a la función que se desempeña en la Administración.

Undécimo. Uso del correo electrónico.

1. El servicio de correo electrónico proporcionado por la Administración permite facilitar la comunicación y colaboración en el ámbito laboral.

2. La Administración dotará a cada usuario de una dirección individual de correo electrónico para su uso en el desempeño de sus funciones. La dirección electrónica personal del empleado público acompañará a éste durante su vida laboral, pudiéndose establecer alias o listas asociadas al mismo en función de su puesto. El personal externo

que colabore eventualmente con la Administración podrá disponer de una cuenta de correo electrónico bajo el dominio @externas.dominiointerno.

3. La Administración podrá utilizar la dirección de correo proporcionada para la comunicación con sus empleados.
4. Si un usuario finaliza su relación funcional o laboral con la Administración se dará de baja su dirección de cuenta de correo.
5. El acceso al correo electrónico se realizará a través de los protocolos pop3, imap y http (interfaz de navegación web) tanto desde la Red Corporativa como desde Internet.
6. La autenticación será al menos a través de usuario y contraseña, modificable ésta por parte del usuario.
7. La Administración podrá determinar el tamaño máximo de los ficheros adjuntos en un correo electrónico y asignar a los usuarios un tamaño de buzón, dentro de unos límites aceptables.
8. Responsabilidades de uso:
 - a) La utilización del servicio de correo electrónico proporcionado por la Administración implica el conocimiento y plena aceptación de las normas de uso y condiciones que se especifican en la presente instrucción y en todos los documentos complementarios de normativa de utilización de servicios y recursos informáticos proporcionados por la Administración.
 - b) Los usuarios son responsables de todas las actividades realizadas con las cuentas de correo electrónico proporcionadas por la Administración y evitarán prácticas que puedan comprometer la seguridad de la información.
 - c) Cada usuario es responsable de salvaguardar sus datos de autenticación y del uso del correo electrónico que se haga a través de la misma.
 - d) El correo electrónico no podrá ser utilizado con fines comerciales ni lucrativos en beneficio del empleado.
9. Se considerarán prácticas no aceptables relacionadas con el uso del correo electrónico:
 - a) El envío o contestación de mensajes o cadenas de mensajes susceptibles de provocar congestiones en los sistemas o que puedan introducir malware o implicar cualesquiera riesgos o problemas en los sistemas y herramientas informáticas y tecnológicas.
 - b) La distribución de mensajes con contenidos no apropiados.
 - c) La falsificación de las cabeceras de correo electrónico.
 - d) La difusión de contenido ilegal.
 - e) El envío de correo electrónico que comprometa la reputación de la Administración a foros de discusión, listas de distribución y/o newsgroups.
 - f) El envío de correo electrónico de forma que suplante u oculte la identidad de otro usuario.
 - g) La definición y uso en el puesto de trabajo de una cuenta de correo adicional de uso no corporativo, tipo pop3/imap.
10. Los mensajes de correo electrónico de los usuarios están protegidos por el derecho a la privacidad y el secreto de las comunicaciones. Cualquier acceso a este tipo de información se realizará exclusivamente para los fines especificados en esta instrucción, previa autorización expresa de la Secretaría General correspondiente o de la Dirección General competente en materia de infraestructuras y servicios comunes de tecnologías de la información y comunicaciones, con notificación expresa al interesado y en presencia del mismo.

Duodécimo. Acceso a las redes de comunicaciones.

1. Toda conexión de los usuarios a cualquier red de comunicación, tanto a la red corporativa de comunicaciones, a Internet, como a otras redes, será facilitada únicamente por la Dirección General competente en materia de infraestructuras y servicios comunes de tecnologías de la información y las comunicaciones.
2. Las conexiones desde redes externas se autorizarán preferiblemente a través de redes privadas, por ejemplo, mediante líneas dedicadas, enlaces punto a punto y similares. Se impondrán restricciones a las direcciones IP desde las que se inicia la conexión, a las direcciones IP a las que se permite realizar la conexión, y cuando sea posible, a la interfaz del equipo de comunicación por la que se recibe dicha comunicación.

3. Toda conexión se realizará con el equipamiento informático facilitado por la Administración para tal fin. El personal externo que colabore con la Administración que deba conectarse a los entornos corporativos desde sus equipos, requerirá una autorización o en su caso la supervisión del responsable de los sistemas de información pertinentes. La Administración podrá establecer sistemas de identificación automática de los equipos que se conectan a cualquiera de sus redes, registrando las conexiones establecidas y el equipamiento conectado.

4. Siempre que se estime necesario por la Secretaría General u órgano equivalente en el resto de organismos dependientes, un usuario podrá acceder a la información desde el exterior mediante el uso de VPN (red privada virtual), que establecerá al menos mecanismos de seguridad como el túnel de cifrado entre origen y destino, el registro de los diferentes accesos y la autenticación de usuario al menos mediante contraseña; para el personal externo se requerirá la firma de un acuerdo de confidencialidad.

5. La Administración podrá desactivar una conexión si se detectan virus o cualquier aspecto técnico que pueda alterar o significar un riesgo para otros sistemas informáticos o servicios de la red. La desactivación se prolongará hasta el momento en el que se confirme que los problemas han sido resueltos.

Capítulo III

Uso de los medios

Decimotercero. Prácticas no aceptables.

Se considerarán prácticas no aceptables:

- a) El uso de los sistemas de información para la comisión de acciones contrarias a sus objetivos o la legislación vigente.
- b) El tratamiento de los activos de información de manera contraria a las pautas definidas por la Administración.
- c) Eludir la autenticación del usuario, revelar la identificación personal de acceso, permitir el uso de la cuenta a otros usuarios o suplantar la personalidad de otro usuario accediendo o haciendo uso de los recursos informáticos de la Administración.
- d) El intento de alterar, evitar o saltar las medidas de seguridad informática configuradas en el equipo entregado.
- e) La desconfiguración del equipo o la modificación del software preinstalado.
- f) La instalación de cualquier software sin autorización expresa.
- g) Ejecutar cualquier forma de análisis o monitorización de la red o equipos, que intercepten datos, a menos que sean parte de las actividades de seguridad autorizadas.

Decimocuarto. Registros de acceso.

1. La Administración guardará en sus servidores, para fines estadísticos, de control del rendimiento del sistema y delimitación de posibles responsabilidades por uso indebido, el registro de los accesos a Internet y las llamadas telefónicas que se produzcan, así como el registro de los mensajes de correo que se envíen. El acceso a estos registros estará limitado a los administradores del sistema de accesos a Internet, a los administradores de comunicaciones y a los administradores de correo respectivamente.

2. De cada uno de los accesos a estos registros se hará la oportuna anotación de quién accede, para qué y cuándo se realiza el acceso. Se guardarán copia de los registros durante un año, a salvo de lo que otras normas legales puedan establecer.

3. En el caso de los accesos a Internet el registro incluirá la información de la dirección desde la que se accedió, página visitada, hora y fecha de la entrada y otros parámetros técnicos necesarios para la prestación del servicio.

4. En el caso de las llamadas telefónicas el registro incluirá el origen, el destino y la duración de la llamada.

5. En el caso de los mensajes de correo enviados el registro contendrá el emisor, el receptor, identificador del mensaje, así como la fecha y hora de paso por el servidor y otros parámetros técnicos necesarios para la prestación del servicio. En ningún caso se conservará el contenido de los mensajes.

6. Previa petición se podrá facilitar a las Secretarías Generales, las estadísticas de uso de la navegación a Internet de los puestos de trabajo de las redes locales de los centros de su competencia así como los datos de los registros telefónicos.

7. Previa solicitud por escrito de una de las partes intervinientes en la comunicación y a través de la Secretaría General correspondiente, los administradores del sistema de correo podrán acceder al registro de correos para solventar posibles controversias sobre la emisión y entrega de mensajes dentro de la propia Administración. Cualquier otro tipo de acceso deberá ser autorizado por la autoridad judicial pertinente.

Decimoquinto. Control y consecuencia del mal uso de los medios tecnológicos.

1. Cada usuario es responsable del equipamiento que la Administración le ha confiado para el desarrollo de sus funciones laborales. Cualquier daño ocasionado por el uso o traslado inadecuado de los recursos, será atribuible al usuario.

2. Los usuarios deberán colaborar con los administradores de sistemas en cualquier investigación que se haga sobre el uso de los recursos, aportando la información que se les requiera.

3. La Administración podrá establecer, por razones específicas de seguridad o de evaluación del desempeño, medidas de control y podrá comprobar, mediante los mecanismos formales y técnicos que estime oportunos, la correcta utilización por parte de los usuarios de todos los sistemas de información, recursos y redes de comunicación puestos a su disposición para el desempeño de sus funciones. Estos controles y revisiones se realizarán respetando los principios de necesidad, idoneidad y proporcionalidad, preservando las garantías del derecho a la intimidad del usuario y la seguridad de las comunicaciones.

4. Sin perjuicio de las posibles responsabilidades penales en que se pudiera incurrir, en caso de que fuera necesario, corresponderá al órgano competente la adopción de medidas disciplinarias hacia los usuarios infractores de esta normativa.

Decimosexto. Responsabilidad específica del personal especializado en tecnologías de la información y las comunicaciones.

El personal que realiza funciones en materia de tecnologías de la información y las comunicaciones ejecutará estas instrucciones siguiendo los principios básicos de deontología profesional, respetando los derechos de los usuarios y el secreto profesional.