BOR nº 76, de 1 de julio de 2016 [página 7861]

Orden 5/2016, de 28 de junio, de la Consejería de Administración Pública y Hacienda, por la que se aprueba la Política de Uso Aceptable de los sistemas de información corporativos de la Comunidad Autónoma de La Rioja

La utilización constante y creciente de las tecnologías de la información y las comunicaciones en el ámbito de la administración pública, tanto para el funcionamiento interno como para la relación con los ciudadanos, supone una clara eficiencia en el uso de los recursos económicos.

Este uso masivo de la tecnología, soportado por dispositivos cada vez más potentes, con mayor capacidad de almacenamiento de información y también con mayores posibilidades de conexión, traen consigo una mayor complejidad de los sistemas y de las redes y un incremento en los riesgos que existen sobre esa información. Se trata no sólo de riesgos de pérdida o fuga de información sino también de riesgos asociados a la pérdida de confidencialidad, a la modificación no autorizada o pérdida de integridad y a la pérdida de disponibilidad u otras amenazas que afectan a información.

Esta extensión de las nuevas tecnologías ha puesto a disposición de las autoridades y de los empleados públicos una serie de recursos informáticos, cuyo empleo debe hacerse de forma ordenada y enfocada al desempeño de su actividad. Por ello, es necesario poner en conocimiento de todo el personal el modo adecuado de utilización de las nuevas tecnologías en el ámbito de la Comunidad Autónoma de La Rioja. De esta forma se hará un uso más eficiente de las mismas, lo que repercutirá positivamente en una más eficiente gestión administrativa y por tanto en un mejor servicio al ciudadano.

Pero además, es necesario prevenir las posibles prácticas abusivas que de una utilización particular de los medios informáticos públicos se pudieran producir, y muy especialmente de aquéllas que puedan llegar a poner en riesgo la seguridad de los sistemas informáticos y, con ello, de las bases de datos que contienen datos personales de los ciudadanos. Esta necesidad de proteger la información generada en el sector público ya motivó la aprobación del Decreto 40/2014, de 3 de octubre, por el que se aprueba la Política de Seguridad de la Información de la Comunidad Autónoma de La Rioja, de la que esta Orden es una manifestación parcial.

Finalmente, también hay que asegurar que el uso de los distintos programas informáticos se haga respetando las condiciones establecidas en sus licencias de uso, garantizando de esta manera los derechos de los proveedores que participan en el desarrollo informático de nuestro sector público.

Para cumplir estas tres finalidades -eficiencia en gestión, seguridad en los datos y respeto a las licencias de uso-, la política de uso aceptable regula las obligaciones de las autoridades y de los empleados públicos de la Comunidad Autónoma en su condición de usuarios de los sistemas tecnológicos puestos a su disposición para el desempeño de sus funciones. Este conjunto de normas implican tanto aspectos de seguridad como organizativos, de protección de datos, de eficiencia y de responsabilidad.

En su virtud, y en uso de las facultades que tengo atribuidas, apruebo la siguiente

Orden

Artículo único. Política de uso aceptable

Primero. Se aprueba la política de uso aceptable de los sistemas de información corporativos de la Comunidad Autónoma de La Rioja, que se incluye como anexo a esta Orden.

Segundo. Todos los usuarios de los sistemas de información y redes de comunicaciones que sean propiedad o estén bajo la supervisión de la Administración General de la Comunidad Autónoma de La Rioja y de sus organismos públicos están obligados al conocimiento y cumplimiento de esta política.

Disposición final única. Entrada en vigor

La presente Orden entrará en vigor a partir de su publicación en el Boletín Oficial de La Rioja.

Logroño a 28 de junio de 2016.- El Consejero de Administración Pública y Hacienda, Alfonso Domínguez Simón.

ANEXO: POLÍTICA DE USO ACEPTABLE DE LOS SISTEMAS DE INFORMACIÓN CORPORATIVOS

1. Principios básicos

Esta política de uso aceptable está basada en una serie de principios básicos con el objeto de garantizar la seguridad de la información en todos sus aspectos.

Los principios básicos sobre los que se asienta esta política son:

a) Principio de máxima seguridad: Todo aquello que no está explícitamente permitido, está prohibido.

b) Principio de control: Los sistemas de información y la red dispondrán de los mecanismos de control, supervisión y registro necesarios para garantizar que el uso que se hace de ellos es el adecuado.

c) Principio de auditoría: Los registros de actividad de los sistemas de información y de la red, se almacenarán durante el máximo tiempo posible para garantizar las máximas posibilidades de auditoría y trazabilidad de las acciones realizadas en los sistemas.

d) Principio de menor autoridad. Los perfiles de usuario se diseñarán con el acceso a la información y recursos imprescindibles para la ejecución de las funciones asignadas.

e) Principio de confidencialidad: La información deberá tratarse con el debido secreto y el celo profesional. Se tendrá especial cuidado con aquella información que esté clasificada como confidencial, sensible, privilegiada o que incluya datos de carácter personal.

f) Principio de eficiencia: Los sistemas de información se usarán de la forma más eficiente posible, evitando gastos o consumos innecesarios.

2. Ámbito de aplicación

La presente política será de aplicación a todos los usuarios de la red corporativa de la Administración General de la Comunidad Autónoma de La Rioja y de sus organismos públicos, conforme a lo dispuesto en el artículo 2 del Decreto 40/2014, de 3 de octubre, por el que se aprueba la Política de Seguridad de la Información de la Comunidad Autónoma de La Rioja.

Se consideran usuarios tanto las autoridades y empleados públicos, como quienes de forma eventual tengan acceso a través de redes y aplicaciones de la Administración autonómica.

No se considerará usuarios de la red corporativa ni quedarán por tanto sujetos a las previsiones de esta Orden quienes hagan uso de las conexiones wifi de cortesía que se ponen a disposición de los ciudadanos en edificios oficiales y centros públicos.

3. Política sobre el uso de equipamiento informático

a) El Gobierno de La Rioja, a través de la Dirección General de las Tecnologías de la Información y la Comunicación, proporcionará a los usuarios, el equipamiento informático adecuado para la realización de las tareas relacionadas con su puesto de trabajo. Este equipamiento es propiedad del Gobierno de La Rioja y su uso debe ir ligado al funcionamiento de los servicios públicos.

b) La Dirección General de las Tecnologías de la Información y la Comunicación definirá la configuración hardware y software de los diferentes equipos y proporcionará los accesos a la red corporativa para cualquier dispositivo. En consecuencia, ningún equipo ni dispositivo deberá ser conectado a la red, si no es por técnicos autorizados de la Dirección General de las Tecnologías de la Información y la Comunicación.

c) Toda la información almacenada en los sistemas de información del Gobierno de La Rioja es de su propiedad y, por tanto, está sujeta a esta Política de Uso Aceptable y a cuantas normas de uso apruebe la organización.

d) El personal de la Dirección General de las Tecnologías de la Información y la Comunicación es el responsable de modificar o alterar la configuración de los dispositivos, tanto a nivel hardware como software. En consecuencia, sólo este personal podrá proceder a instalar o desinstalar cualquier tipo de software de un dispositivo de uso corporativo. En consecuencia, los usuarios no dispondrán de autorización de administración sobre los equipos, salvo autorización expresa de la Dirección General de las Tecnologías de la Información y la Comunicación

e) Por razones de seguridad y de protección de derechos de propiedad intelectual no está permitida la instalación de ningún software protegido por derechos de autor o con licencia, sin que se disponga de la misma.

f) La Dirección General de las Tecnologías de la Información y la Comunicación es responsable del inventario de equipamiento informático de la organización, sin perjuicio de las competencias de la Dirección General competente en materia de Patrimonio.

g) Cualquier equipo o recurso deberá usarse de la forma más eficiente posible. En consecuencia deberá:

- Apagar el equipo y la impresora local si la hubiera, al terminar la jornada.
- Imprimir o copiar únicamente aquellos documentos que sea necesario en el marco de la gestión pública, a ser posible a doble cara y evitando en la medida de lo posible el uso de los sistemas de impresión de color.
- Usar preferentemente impresoras en red o equipos multifuncionales a equipos personales y equipos láser a equipos de inyección de tinta.
- Utilizar los recursos de almacenamiento compartido (unidades e red) para almacenar la información que sea estrictamente necesario mantener.

4. Política de gestión de usuarios e identificación y autenticación

a) Cualquier usuario con acceso a los sistemas de información deberá disponer de una identificación personalizada (identificador de usuario).

b) Los responsables de personal de cada unidad o servicio son los responsables de notificar a la Dirección General de las Tecnologías de la Información y la Comunicación cualquier modificación que se produzca a este respecto (altas y bajas o cambios de perfil), con el objetivo de garantizar que el listado de usuarios con acceso y privilegios se encuentra permanentemente actualizado.

c) Para el acceso a los sistemas, el usuario deberá utilizar su nombre de usuario y su contraseña de acceso.

d) En función de la adecuación del sistema o de la aplicación, podrá requerirse otro sistema de autenticación que permita la identificación fehaciente del usuario, como es el caso del Certificado Digital.

e) En el caso de las contraseñas, la Dirección General de las Tecnologías de la Información y la Comunicación se establecerá una política general de fortaleza de la contraseña (longitud mínima y complejidad) así como un periodo de validez máxima pasado el cual deberá, necesariamente, ser cambiada. El usuario deberá ser el único conocedor y responsable de la custodia de la contraseña. No debe facilitarse la contraseña de acceso a ningún otro usuario ni siquiera a los técnicos responsables del soporte. El usuario dispondrá de la posibilidad de cambiar su contraseña de acceso cuando lo considere oportuno.

f) En caso de sospecha de acceso no autorizado, el usuario deberá proceder al cambio de contraseña de forma inmediata. Este acceso no autorizado será considerado como un incidente de seguridad que será tratado tal como se establece en el apartado 6.

g) Al abandonar de forma temporal el puesto de trabajo, se deberá proceder al bloqueo del dispositivo. Al hacerlo al finalizar la jornada, se deberá proceder al apagado completo.

5. Política del servicio de soporte y mantenimiento

a) La Dirección General de Tecnologías de la Información y la Comunicación es la responsable de proporcionar el soporte informático necesario para todas las incidencias relacionadas con las tecnologías de la información y la comunicación. Para garantizar una máxima eficiencia en este servicio de soporte, desde la Dirección General de las Tecnologías de la Información y la Comunicación se podrá supervisar proactivamente los equipos, programas y redes de comunicaciones que se precisen. La supervisión se llevará a cabo respetando los criterios de necesidad, idoneidad y proporcionalidad, y de conformidad con los siguientes requisitos:

   1) Que se hayan establecido previamente las reglas de uso de los medios informáticos puestos a disposición del trabajador -prohibiciones absolutas o parciales-.

   2) Que se informe a los trabajadores de que va a existir control sobre dichos medios.

   3) Que igualmente se informe a los trabajadores de los medios de control que van a ser usados para fiscalizar el uso de los medios informáticos.

b) Cualquier solicitud de ayuda o de soporte deberá hacerse, en primera instancia, al Centro de Atención a Usuarios del Gobierno de La Rioja, utilizando los canales establecidos al respecto (teléfono y portal web).

c) En la medida de lo posible, el soporte técnico se realizará de forma remota, utilizando las herramientas que desde la Dirección General de las Tecnologías de la Información y la Comunicación se consideren convenientes. Estas herramientas deberá garantizar la confidencialidad del trabajo del usuario para lo que se requerirá siempre de la aceptación de la conexión por parte del interesado.

6. Gestión de incidentes de seguridad de la información

De acuerdo con la legislación vigente y con las buenas prácticas del mercado, el Gobierno de La Rioja deberá gestionar cualquier incidente que afecta a la seguridad de la información, para ello se establece la siguiente política:

a) Cualquier incidente de seguridad que comprometa la información de la organización, deberá ser notificado con el objeto de establecer las medidas de contención y/o recuperación de la forma más rápida posible.

b) Los incidentes de seguridad que afecten a datos de carácter personal deberán ser notificados al responsable del fichero.

c) El usuario deberá notificar estas incidencias al Centro de Atención a Usuarios, que a su vez, iniciará los procedimientos de restauración, notificación o contención de la amenaza. La Dirección General de las Tecnologías de la Información y la Comunicación será responsable de establecer al protocolo de notificación de estos incidentes.

7. Manejo de información

La actividad administrativa genera múltiple información de considerable utilidad. En algunos casos, dicha información es pública y se pone a disposición de los ciudadanos mediante publicación en diferentes formatos. Sin embargo, en otras ocasiones, esa información contiene datos de carácter personal, de naturaleza protegida, o incluso datos confidenciales con protección reforzada, como los que afectan a la salud de las personas o los de naturaleza tributaria. La tenencia de estos datos genera en la Comunidad Autónoma de La Rioja, como organización, la obligación de protegerlos. Y para ello, es obligación de los empleados públicos y autoridades de la administración ayudar a preservarla mediante un manejo adecuado de la información, evitando riesgos de alteración no controlada, pérdida o acceso no autorizado. Por ello:

a) Se deberá prestar especial atención a la información procedente de fuera de la organización sea cual sea el mecanismo de acceso (correo electrónico, dispositivos de almacenamiento USB, discos 'cloud'...).

b) El uso de sistemas o servicios de almacenamiento en la nube (Dropbox, BOX; Google drive...) exigirá previa autorización de la DGTIC.

c) No debe sacar información de carácter personal del centro de trabajo a menos que disponga de la correspondiente autorización de movimiento tanto de entrada como de salida de soportes por parte del responsable del fichero.

d) Cada usuario es responsable de la seguridad de la información almacenada en los dispositivos que tenga asignados. Desde la Dirección General de las Tecnologías de la Información y la Comunicación se establecerá un procedimiento de copia de seguridad de los datos alojados en las unidades de red de los servidores de ficheros corporativos (unidades V, W, X...).

e) Con carácter general, el uso de memorias USB en la organización deberá limitarse a los casos en los que sea imprescindible. Por esta razón, en los puestos de usuario se procederá a deshabilitar los dispositivos de almacenamiento masivo en los puertos USB. Su habilitación deberá justificarse por el usuario y requerirá autorización del jefe de servicio antes de ser aprobado por la Dirección General de las Tecnologías de la Información y la Comunicación.

f) La Dirección General de las Tecnologías de la Información y la Comunicación dispone ya de varios sistemas alternativos al uso de memorias USB que deberán ser valorados por el usuario antes de solicitar la habilitación del puerto USB del equipo.

g) En las unidades de red no podrán almacenarse más archivos que los necesarios para la prestación de las funciones encomendadas, para no perjudicar el rendimiento del servicio y evitar costes de almacenamiento.

h) Desde la Dirección General de las Tecnologías de la Información y la Comunicación se facilitará el correspondiente software antivirus para la protección contra virus informáticos. Es obligatorio que dicho programa se encuentre funcionando y actualizado de forma permanente. En ningún caso podrá procederse a la detención de dicho servicio.

i) Ante la presencia de cualquier fichero que le resulte sospechoso, proceda a analizarlo con el antivirus. No debe abrir un fichero sospechoso bajo ningún concepto. Si tienen dudas, póngase de inmediato, en contacto con el Centro de Atención a Usuarios.

8. Seguridad de los dispositivos móviles

Se entiende por dispositivo móvil todo aquel dispositivo con capacidad de proceso que puede ser fácilmente transportado de un lugar a otro y que dispone de algún sistema de conexión a la red corporativa. Entre estos dispositivos se encuentran los ordenadores portátiles, las tabletas de cualquier tipo y sistema operativo y los denominados teléfonos inteligentes o smartphones.

En comparación con los ordenadores de sobremesa, los dispositivos móviles requieren, en general, medidas de seguridad adicionales, debido a que suelen estar expuestos a un mayor número de riesgos de distinta naturaleza, especialmente los derivados de su uso fuera de las instalaciones de la organización, obligando a considerar incidentes tales como el uso de redes wifi inseguras, el extravío o el hurto.

También hay que considerar los problemas añadidos cuando se trata de dispositivos propiedad de los propios usuarios, puesto que tales equipos pueden presentar importantes inconvenientes en materia de seguridad derivados tanto de su configuración como de un uso inseguro.

Además, la mayoría de las aplicaciones que se ejecutan en dispositivos móviles se descargan de tiendas de aplicaciones, tanto oficiales como no oficiales, e incluso de páginas web. Aunque, en algunos casos, las tiendas realizan controles limitados respecto de las aplicaciones de terceros que albergan, no puede obviarse el riesgo adicional para los usuarios finales. Los dispositivos móviles también pueden acceder a información a través de métodos característicos de estas plataformas, como los códigos QR que llevan a direcciones URL a través de las cámaras.

Los servicios de localización suponen un riesgo adicional, toda vez que posibilitan a los atacantes determinar la posición del usuario en función de la localización de su dispositivo móvil, lo que puede afectar ya no sólo a la seguridad de la organización sino también a las garantías de privacidad del propio usuario, facilitando la creación de mapas geográficos de los movimientos de los usuarios y, en algunos casos, el tipo de actividad que desarrolla.

Debido a todos los factores descritos, es necesario adoptar las siguientes medidas de seguridad en tanto tales equipos tengan acceso a aplicaciones o datos corporativos:

a) Mientras los mecanismos de seguridad no lo permitan, solo podrán conectarse a la red corporativa aquellos dispositivos que sean gestionados por la Dirección General de las Tecnologías de la Información y la Comunicación. Esto significa que no podrá conectarse a la red corporativa ningún dispositivo de uso personal y privado.

b) La Dirección General de las Tecnologías de la Información y la Comunicación será responsable de la entrega e inventariado del dispositivo que se asigne a cada usuario. El usuario será responsable del correcto uso y custodia tanto del dispositivo como de la información que almacena.

c) El acceso a cualquier dispositivo móvil se protegerá con una contraseña o patrón. Para evitar el acceso sencillo a la información almacenada en el dispositivo en caso de extravío.

d) La Dirección General de las Tecnologías de la Información y la Comunicación podrá instalar sistemas de control en los dispositivos móviles, con objeto de mejorar la seguridad de la información de los mismos. Estos sistemas de control dispondrán de la posibilidad de imponer políticas de seguridad sobre el dispositivo y de un mecanismo de borrado remoto.

e) En caso de extravío de un dispositivo, deberá procederse al borrado completo de la información del mismo utilizando las herramientas del fabricante o notificando a la Dirección General de las Tecnologías de la Información y la Comunicación el incidente de seguridad que hará uso de las medidas recogidas en el punto anterior.

f) No está permitido desinstalar los programas o herramientas de seguridad de los dispositivos móviles.

g) La información de carácter personal, sensible o clasificada, almacenada en dispositivos móviles deberá estar cifrada. Es responsabilidad del usuario realizar el cifrado de esta información para evitar el acceso no autorizado a la misma.

9. Uso del correo electrónico

El correo electrónico es hoy en día uno de los mecanismos de intercambio de información más utilizados, tanto en el ámbito personal como en el profesional. Todas las personas que utilizan Internet en su trabajo o en su hogar disponen de una o más cuentas de correo electrónico, cuentas que sufren a diario ataques de todo tipo con el objetivo principal de robar información.

El uso del correo corporativo de forma que se degrade la imagen de la organización no es habitual, pero debemos tener en cuenta que un uso inadecuado de las direcciones de correo electrónico propias del Gobierno de La Rioja pueden perjudicar seriamente a su imagen: si un usuario envía correos insultantes, de contenido ilícito, que fomenten actitudes contrarias a la convivencia no sólo se perjudicará la imagen de esta persona, sino la de la organización en su conjunto; de esta forma, nuestra política de uso del correo electrónico debe reflejar claramente la prohibición del uso del correo corporativo con estos fines, minimizando así tanto la probabilidad como el impacto asociados al riesgo reputacional en el uso del correo.

El correo electrónico es un medio habitual de propagación de bulos (hoaxes), noticias falsas que intentan pasar por reales ante sus receptores. A diferencia de los fraudes, como el phising, los bulos no tienen por qué tener propósito delictivo o de lucro, aunque pueden implicar impactos muy dañinos contra una organización. El envío de un bulo puede ser el medio para cometer un ataque de ingeniería social, de envío de software dañino, de recopilación de direcciones de correo electrónico, de incremento malicioso del tráfico o incluso un ataque severo. En cualquier caso, con independencia de su fin último, los bulos deben considerarse un riesgo potencial para la seguridad corporativa.

El correo electrónico es probablemente la herramienta de trabajo que mueve más información entre usuarios de la organización y con usuarios externos y, en cuanto herramienta de trabajo corporativa propiedad de la institución y sujeta a las vulnerabilidades y riesgos descritos y a otros que se generan cada día, conviene establecer las siguientes directrices para su uso.

La utilización del servicio de correo electrónico proporcionado por el Gobierno de la Rioja implica el conocimiento y plena aceptación de esta Política de Uso.

a) El usuario utilizará el Correo Corporativo de acuerdo con la ley, la moral y buenas costumbres generalmente aceptadas y el orden público, y se comprometerá a no emplearlo para incurrir en actividades ilícitas, ilegales o contrarias a la buena fe. Se abstendrá de difundir contenidos o propaganda de carácter racista, xenófobo, de apología del terrorismo, pornográfico y, en general, contrario o atentatorio a los derechos humanos, a las libertades públicas reconocidas constitucionalmente y al derecho al honor, a la intimidad personal y familiar y a la propia imagen de las personas, de conformidad con los principios éticos y reglas de conducta definidos en los artículos 53 y 54 del Texto Refundido de la Ley del Estatuto Básico del Empleado Público.

b) El Gobierno de la Rioja 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 y será intransferible.

c) Cuando un usuario finalice su relación funcionarial o laboral con la Administración se procederá a la cancelación del buzón de correo electrónico.

d) El acceso al correo electrónico se realizará en general, a través de interfaz que se determine. Podrá accederse al correo electrónico del Gobierno de La Rioja tanto desde la red corporativa como desde fuera de la misma. La Dirección General de las Tecnologías de la Información y la Comunicación se encargará de establecer las medidas técnicas razonables para asegurar la seguridad del acceso desde fuera de la red corporativa.

e) El acceso al correo electrónico requerirá identificación previa del usuario. Dicha identificación podrá realizarse de forma automática tras haberse identificado como usuario de la red (dominio) o realizarse de forma expresa. El usuario podrá cambiar su contraseña cuando desee. Este cambio puede conllevar el cambio de la contraseña en otras aplicaciones como el Dominio Microsoft. Las contraseñas son personales e intransferibles, y por lo tanto deben mantenerse en secreto.

f) Queda expresamente prohibido el envío a través del correo corporativo de información sensible hacia direcciones de correo personales, incluso aunque tales direcciones pertenezcan al propio usuario.

g) La DGTIC determinará el tamaño máximo de los ficheros adjuntos en un correo electrónico y asignará a los usuarios un tamaño de buzón, dentro de unos límites aceptables. Asimismo y por razones de seguridad se limitará el número máximo de destinatarios que pueden recibir un mensaje.

h) Cada usuario será responsable de todas las actividades realizadas a través de las cuentas de correo electrónico proporcionadas por la Administración.

i) El correo electrónico corporativo no podrá ser utilizado con fines comerciales ni lucrativos en beneficio del empleado público de conformidad con la legislación básica estatal en materia de función pública.

j) El usuario no deberá responder a correos no solicitados y de origen desconocido. No actuar así aumenta la cantidad de correo basura en los buzones. Los mensajes no deseados o que no requieran ningún tipo de acción deberán borrarse lo antes posible para evitar problemas de almacenamiento. Se recomienda por tanto no almacenar mensajes y archivos de correo que no se consideren necesarios.

k) Aunque el sistema de correo del Gobierno de la Rioja realiza un control antivirus de los correos recibidos, no deberá abrir nunca correos sospechosos (respuestas a mensajes que no se enviaron, correos de origen desconocido, etc.) ni tampoco deberá abrir los ficheros adjuntos ni hacer clic en sus enlaces. Estos mensajes tienen una alta

probabilidad de incluir o contener malware y por tanto de ocasionar pérdidas de información, que pueden llegar a ser muy cuantiosas e irreparables.

l) No se deberán reenviar ni crear cadenas de mensajes.

m) No se debe proporcionar la dirección de correo en sitios web, foros de discusión, listas de distribución, etc... que puedan comprometer la imagen o la reputación del Gobierno de la Rioja. Cualquier acción en sentido contrario será responsabilidad exclusiva del usuario.

n) El empleado cuidará en todo momento el lenguaje utilizado en sus correos institucionales, debiendo tener presente que en cada uno de ellos representa la imagen y el nombre de la Comunidad Autónoma de La Rioja.

o) En caso de enviar un correo electrónico a múltiples destinatarios, especialmente cuando estos destinatarios son externos, deberá utilizar el campo de envío CCO (con copia oculta), para evitar dar a conocer las direcciones de terceras personas a menos que sea imprescindible.

p) Los mensajes de correo electrónico de los usuarios están protegidos por el derecho a la privacidad y el secreto de las comunicaciones. No se prevé el acceso al contenido de un buzón a no ser por el interesado, salvo que dicho acceso sea solicitado por los tribunales de justicia o cuando exista una sospecha fundada de comisión de un delito. En estos casos al acceso se realizará con el máximo de garantías legales.

Debe recordar que el correo electrónico no es un sistema de archivo de información por lo que no debe usarse como tal. La organización dispone de herramientas diseñadas y dedicadas a este efecto como son los servidores de archivos.

Debe recordar también que el correo electrónico no garantiza la entrega de un mensaje ni tiene por qué notificar el error en la entrega incluso aunque se utilice la opción de 'acuse de recibo'. No debe utilizarse, por tanto, como un sistema de notificaciones.

10. Acceso a Internet

Cada día se hace más necesario disponer de conexión con la red internet para el acceso a recursos e información en fuentes abiertas. Sin embargo, también se hace igualmente necesario establecer unas medidas que nos protejan del creciente número de amenazas que proliferan en la red. Estas medidas deben ir encaminadas a garantizar la seguridad de la información de la organización. La Dirección General de las Tecnologías de la Información y la Comunicación establecerá las medidas de seguridad razonables para minimizar el riesgo de la conexión con internet y para garantizar la auditoría de los accesos a esa red.

a) La conexión a la red Internet obedece a fines profesionales y por tanto debe ser utilizada como tal.

   La utilización de dispositivos USB, teléfonos móviles u otros elementos, como acceso alternativo a Internet, sólo podrá realizarse previa autorización de la Dirección General de las Tecnologías de la Información y la Comunicación.

b) Cualquier uso que pueda provocar una pérdida de calidad en el servicio para el resto de usuarios, deberá limitarse. Entre estas acciones está la subida y/o descarga de grandes ficheros multimedia. Este tipo de ficheros son de un tamaño muy grande que pueden colapsar no solo la conexión a internet sino también la red interna.

c) La conexión a redes sociales sólo procederá cuando la naturaleza del puesto de trabajo lo requiera.

d) No está permitido el acceso a contenidos inadecuados como aquellos con contenido violento, sexual, xenófobo o similar, ni a aquellos que puedan suponer un riesgo para la seguridad de la información (páginas de hacking o similares). La Dirección General de las Tecnologías de la Información y la Comunicación establecerá unas medidas de seguridad razonables para controlar o bloquear este tipo de contenidos.

e) No está permitido el acceso a redes anónimas que dificulten la trazabilidad de las actividades o el uso de sistemas o programas cuyo objetivo sea evitar los sistemas de control y seguridad de la organización en el acceso a internet. Algunas de estas actividades puedes ser constitutivas de delito y están recogidas en el código penal.

f) No puede utilizarse material protegido por propiedad intelectual o industrial sin permiso del propietario. Es responsabilidad de cada usuario la comprobación de derechos de propiedad intelectual y/o industrial de cada archivo o programa que se descargue o utilice. En caso de contravenir esta norma el usuario estará sometido a las previsiones disciplinarias, administrativas, civiles o penales descritas en las leyes.

g) Se establecerá un mecanismo que permita registrar las acciones llevadas a cabo por cada usuario con el objeto de proceder a realizar los correspondientes análisis de seguridad, de acuerdo con lo previsto en el apartado 5.1.a), y poner esta información en manos de los Cuerpos y Fuerzas de Seguridad del Estado.

11. 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, 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 y requisitos indicados en el apartado 5.a, 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.

12. 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 esta política siguiendo los principios básicos de deontología profesional, respetando los derechos de los usuarios y el secreto profesional.

13. Control y supervisión

La Dirección General de las Tecnologías de la Información y la Comunicación será la encargada de establecer y mantener los sistemas de seguridad para proteger la información.

Si el personal de soporte técnico de la Dirección General de las Tecnologías de la Información y la Comunicación detectase cualquier anomalía que indicara una utilización de los recursos contraria a la presente norma, lo pondrá en conocimiento de sus responsables, que tomarán las oportunas medidas correctoras y, si fuera necesario, dará traslado de la incidencia a los superiores jerárquicos del usuario.

14. Procedimientos Operativos de Seguridad

La Dirección General de las Tecnologías de la Información y la Comunicación podrá ampliar o completar esta Política de Uso Aceptable mediante la elaboración de Procedimientos Operativos de Seguridad específicos en función de la materia y del momento.

Estos procedimientos Operativos regularán el uso de determinados servicios que, por la causa que fuera, se considere que pudiera suponer un riesgo para la seguridad de la información.

Los Procedimientos Operativos de Seguridad serán publicados en la Intranet del Gobierno de La Rioja y serán también de obligado cumplimiento.

15. Revisión y evaluación

La gestión de esta Política corresponde a la Dirección General de las Tecnologías de la Información y la Comunicación, que es competente para:

a) Interpretar las dudas que puedan surgir en su aplicación.

b) Proponer su revisión, cuando sea necesario para actualizar su contenido.

c) Verificar su efectividad.