

7.5.VARIOS

CONSEJERÍA DE PRESIDENCIA Y JUSTICIA

CVE-2016-6831 *Orden PRE/48/2016, de 22 de julio, por la que se regulan las normas de seguridad sobre utilización de los recursos y sistemas tecnológicos y de información en la Administración de la Comunidad Autónoma de Cantabria.*

Los recursos y sistemas tecnológicos y de información son elementos esenciales para el desarrollo de las misiones encomendadas a la Administración de la Comunidad Autónoma de Cantabria. Su correcta utilización permite trabajar de manera eficaz, eficiente y con un uso racional del dinero público, características que facilitan la prestación de unos servicios de calidad a la ciudadanía, entre los que cabe destacar los recogidos en la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, cuyo contenido ha sido recientemente derogado, al ser actualizado e incluido en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

Por su parte, 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, tiene como finalidad la creación de las condiciones necesarias de confianza en el uso de los medios electrónicos que permita a los ciudadanos y a las Administraciones Públicas el ejercicio de derechos y el cumplimiento de deberes a través de ellos.

Entre las medidas de seguridad obligatorias que establece este Real Decreto, está la creación de una normativa de seguridad que contemple entre otros aspectos, y de forma destacada, el uso correcto de los equipos y servicios, así como lo que se considera uso indebido y las responsabilidades respecto al cumplimiento o violación de las normas de seguridad.

En su artículo 5 señala que "la seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos relacionados con el sistema", lo que incluye tanto al personal especialista en tecnología, a los usuarios de los recursos y sistemas tecnológicos y de información, así como a los responsables con capacidad de decisión sobre su utilización y el acceso a la información que contienen. En ese mismo artículo se fija que "Se prestará la máxima atención a la concienciación de las personas y a sus responsables jerárquicos".

Su artículo 14 trata de forma específica la gestión del personal, señalando que "todo el personal relacionado con la información y los sistemas deberá ser formado e informado de sus deberes y obligaciones en materia de seguridad".

Así, la presente orden establece las reglas sobre los usos aceptables de recursos y sistemas tecnológicos y de información, así como de la información en ellos contenida, con el objetivo de preservar en todo momento las dimensiones de la seguridad que fija el Esquema Nacional de Seguridad: disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad.

El conjunto de normas de seguridad recogidas en la presente orden se han elaborado con el máximo respeto a los derechos constitucionales a la intimidad y la inviolabilidad de las comunicaciones, y sirve para desarrollar la Política de Seguridad de la Información de la Administración de la Comunidad Autónoma de Cantabria.

LUNES, 1 DE AGOSTO DE 2016 - BOC NÚM. 147

DISPONGO

Artículo 1. Objeto.

El objeto de la presente orden es establecer las normas de seguridad sobre utilización de los recursos y sistemas tecnológicos y de información de la Administración de la Comunidad Autónoma de Cantabria, así como de la información que contienen, fijando los usos legítimos, los indebidos y las responsabilidades relativas al cumplimiento o violación de estas normas de seguridad.

Artículo 2. Ámbito de aplicación.

1. Sus previsiones serán de aplicación:

a) A la Administración de la Comunidad Autónoma de Cantabria, comprendiendo ésta, a estos efectos, a la Administración General y los organismos públicos y entidades de derecho público vinculadas o dependientes de la misma, cuando ejerzan funciones administrativas y/o utilicen sistemas tecnológicos o de información gestionados por el órgano directivo con competencias en materia informática. Quedan excluidos del ámbito de aplicación del presente decreto el Servicio Cántabro de Salud y el sector público empresarial y fundacional, salvo cuando utilicen sistemas tecnológicos o de información gestionados por el órgano directivo con competencia en materia informática.

b) A las personas físicas, jurídicas y entes sin personalidad jurídica en sus relaciones con las entidades anteriores cuando procedan al uso de sistemas tecnológicos o de información gestionados por el órgano directivo con competencias en materia informática.

2. Quedan excluidos de la presente orden los ciudadanos que ejerzan sus derechos o cumplan sus deberes mediante los servicios de Administración Electrónica, sin perjuicio de las normas de seguridad o condiciones que pudieran establecerse específicamente para ese caso.

Artículo 3. Uso de recursos y sistemas tecnológicos y de información.

1. La Administración de la Comunidad Autónoma de Cantabria facilitará a los empleados públicos que así lo precisen los equipos informáticos y dispositivos de comunicaciones, tanto fijos como móviles, necesarios para el desempeño de sus funciones.

2. Así mismo, se podrá poner a disposición del personal ajeno a la Administración General de la Comunidad Autónoma de Cantabria y los organismos públicos y entidades de derecho público vinculadas, los medios técnicos que sean necesarios para permitir el acceso a sus recursos y sistemas tecnológicos o de información, siempre en condiciones de seguridad, y exclusivamente destinados al desarrollo del acuerdo o contrato en que se encuadra su vínculo con la Administración de la Comunidad Autónoma de Cantabria.

3. En todos los casos, los datos, dispositivos, programas y servicios tecnológicos que la Administración de la Comunidad Autónoma de Cantabria pone a disposición de los usuarios deben utilizarse para fines profesionales y dentro del desarrollo de las funciones encomendadas.

Artículo 4. Asignación de credenciales de acceso.

1. Todos los usuarios deberán autenticarse mediante los mecanismos de control de accesos provistos en cada sistema.

2. Cada usuario de esos sistemas debe disponer de un identificador único y personalizado, que estará vinculado a las credenciales de acceso que se le entreguen.

3. El uso de un mismo identificador por varios usuarios estará prohibido, salvo en aquellos casos excepcionales en el que esté justificado y autorizado expresamente por el responsable de la información o responsable del servicio afectado. Será preceptivo un informe elaborado por el Responsable de Seguridad de la Información sobre la situación, riesgos y posibles consecuencias y además se aplicarán las medidas de seguridad adicionales que sean necesarias para garantizar la seguridad de los recursos, los sistemas y la información que contienen.

CVE-2016-6831

Artículo 5. Uso de las credenciales de acceso.

1. Cada usuario será responsable de las actividades realizadas con las credenciales de acceso que reciba para acceder a los sistemas y/o recursos.
2. Queda prohibido comunicar o ceder de cualquier modo las credenciales de acceso a los sistemas tecnológicos o de información de la Administración de la Comunidad Autónoma de Cantabria.
3. El usuario deberá adoptar las debidas precauciones en la custodia de las credenciales de acceso asignadas para evitar que terceras personas puedan tener acceso a las mismas.
4. Si un usuario sospecha que sus credenciales son conocidas o están siendo usadas por otra persona o entidad deberá comunicar un incidente de seguridad, poniendo el hecho en conocimiento del órgano directivo competente en materia de informática.

Artículo 6. Usos aceptables de los equipos tecnológicos.

1. Los equipos tecnológicos se usarán para fines profesionales y como herramienta de apoyo a las tareas encomendadas en función del puesto de los usuarios autorizados.
2. Los usuarios facilitarán al personal de soporte técnico el acceso a sus equipos, o la cesión, para labores de reparación, instalación o mantenimiento.
3. Se evitarán comportamientos de riesgo para impedir el acceso y difusión de malware en los equipos, en particular, no se ejecutarán archivos adjuntos a correos ni aplicaciones provenientes de terceras partes que no sean de confianza o desconocidas.
4. Cuando los equipos no se estén utilizando, deberán ser bloqueados para evitar su uso por personas no autorizadas. Si el periodo va a ser prolongado, por razones de seguridad y eficiencia energética, deberán apagarse. En el caso de dispositivos móviles, pasarán a un modo de bajo consumo con bloqueo de terminal.

Artículo 7. Precauciones adicionales para dispositivos móviles o portátiles.

1. En dispositivos móviles o portátiles se evitará almacenar información de forma permanente y se eliminarán periódicamente datos innecesarios.
2. Si fuera necesario el almacenamiento de información confidencial o reservada, el disco duro o memoria interno no volátil donde se almacene estarán cifrados y la información se eliminará cuando deje de ser necesaria.

Se entenderá por información confidencial, aquella a la que se ha tenido acceso por ostentar una autorización específica al respecto, y por información reservada aquella que exclusivamente debe ser difundida entre un conjunto de personas determinadas previamente y para cada caso por los órganos superiores y directivos de la Administración de la Comunidad Autónoma de Cantabria.
3. Se evitará exponer las credenciales de acceso a riesgos innecesarios, en concreto, se evitará almacenar contraseñas en archivos fácilmente accesibles, que los navegadores de Internet las recuerden automáticamente o tenerlas anotadas junto al dispositivo.
4. Los dispositivos móviles o portátiles deberán vigilarse adecuadamente en los lugares públicos para evitar su posible robo o pérdida.

Artículo 8. Usos prohibidos de los equipos tecnológicos.

1. Está específicamente prohibido realizar actividades que puedan poner en riesgo la seguridad de los equipos, las redes, los sistemas o la información que contienen y en particular:
 - a) Alterar cualquier componente físico o lógico o la configuración de los equipos, así como utilizar técnicas del tipo "hackear", "liberar" o equivalentes.
 - b) Utilizar cualquier tipo de software dañino o que haga un uso abusivo de la red o los recursos.

c) Acceder a contenidos o ejecutar de manera remota archivos que puedan suponer un riesgo para la seguridad.

d) Conectar a la red informática corporativa cualquier equipo o dispositivo no facilitado por la Administración de la Comunidad Autónoma de Cantabria o para el que no se haya recibido una autorización expresa de conexión.

e) Utilizar para el uso o acceso de recursos o sistemas de la Administración de la Comunidad Autónoma de Cantabria, y al margen del servicio de teletrabajo proporcionado por la propia Administración, conexiones y medios inalámbricos con tecnologías WiFi, Bluetooth o infrarrojos, o cualquier otra de similares características, que no estén expresamente autorizados.

2. En los equipos corporativos está, además, específicamente prohibido:

a) Utilizar programas informáticos que no hayan sido expresamente verificados y aprobados, incluidos programas portables.

b) Emplear medios de conexión a Internet alternativos a los autorizados expresamente.

3. Está prohibida la reproducción, modificación, transformación, cesión, comunicación o uso fuera del ámbito de la Administración de la Comunidad Autónoma de Cantabria de los programas y aplicaciones informáticas instaladas en los equipos.

4. Está prohibida la transmisión, distribución o almacenamiento de cualquier material obsceno, difamatorio, amenazador o que constituya un atentado contra la dignidad de las personas.

Artículo 9. Habilitación del uso de soportes del almacenamiento extraíbles.

1. Inicialmente, y por defecto, todos los equipos informáticos de usuario corporativos tendrán deshabilitada la posibilidad de utilizar soportes extraíbles.

2. En cada unidad organizativa de nivel jerárquico Servicio, o superior, o también puestos de trabajos singularizados equivalentes, se dejará un equipo con acceso a los soportes extraíbles habilitados. Inicialmente el equipo donde se dejara habilitado será el utilizado por el titular de la unidad o puesto de trabajo singularizado, si bien se podrá solicitar su cambio por el de otro equipo utilizado por otra persona de la misma unidad.

3. Adicionalmente, y siempre que esté debidamente justificado, podrá solicitarle la habilitación del acceso a soportes extraíbles para otros empleados públicos en los siguientes supuestos:

a) Cuando esté justificado en virtud del cumplimiento de las funciones propias del puesto de trabajo.

b) De forma temporal para cualquier empleado público, cuando se corresponda con un uso justificado.

4. En el caso de que sea necesario utilizar dispositivos extraíbles por personal ajeno a la Administración de la Comunidad Autónoma de Cantabria, su uso deberá estar debidamente justificado y ser solicitado por el responsable del órgano o unidad responsable del acuerdo o contrato dentro del cual desarrolla su actividad.

Artículo 10. Normas de uso de soportes del almacenamiento extraíbles.

1. Los usuarios que tengan habilitada la utilización de soportes extraíbles le darán un uso profesional y deberán velar porque los soportes extraíbles que utilicen no supongan un riesgo para la seguridad, evitando cualquier utilización que pueda contaminarlos con virus o cualquier tipo de código malicioso. También deberán procurar no extraviarlos.

2. Si al utilizar un soporte extraíble un usuario percibe indicios de que puede estar contaminado o suponer un riesgo para la seguridad, deberá abstenerse de usarlo y proceder a notificar un incidente de seguridad.

3. Si el soporte extraíble se utiliza para contener información confidencial o reservada, deberá estar cifrado y cumplir con las normas de seguridad sobre clasificación e identificación

LUNES, 1 DE AGOSTO DE 2016 - BOC NÚM. 147

de la información que se establezcan. Si un soporte con ese tipo de información es extraviado, deberá notificarse un incidente de seguridad.

4. Se deberán respetar las medidas de seguridad específicas que puedan establecerse sobre el uso de soporte extraíbles o sobre su retirada.

Artículo 11. Usos aceptables de las comunicaciones electrónicas informativas, en especial del correo electrónico.

1. Los usuarios que lo precisen para el desempeño de sus funciones, dispondrán de una cuenta de correo electrónico para el envío y recepción de mensajes internos o externos a la organización, según sus necesidades.

2. Las herramientas y programas de correo electrónico suministrados, instalados y configurados por la Administración de la Comunidad Autónoma de Cantabria únicamente podrán utilizarse para fines profesionales.

3. No deberán abrirse ni ejecutarse ficheros de terceras que no sean de confianza o desconocidas, puesto que podrían contener virus o código malicioso.

4. Los usuarios deberán asegurarse de que los reenvíos de mensajes previamente recibidos se transmitan únicamente a los destinatarios apropiados.

Artículo 12. Usos prohibidos de las comunicaciones electrónicas informativas, en especial del correo electrónico.

1. Quedan prohibidos aquellos usos del correo electrónico corporativo que puedan perjudicar al funcionamiento o a la seguridad de los sistemas tecnológicos o de información y a la información en ellos contenida, y en particular:

- a) El envío de virus y código malicioso en general.
- b) La utilización del correo corporativo como medio de intercambio de ficheros especialmente voluminosos, según los estándares de uso habituales.
- c) El envío de correos a más de 50 usuarios sin autorización.
- d) La utilización del correo corporativo para recoger correo de buzones que no pertenezcan a la Administración de la Comunidad Autónoma de Cantabria o el reenvío automático del correo corporativo a buzones ajenos a la organización sin la debida autorización.
- e) La difusión de la cuenta de correo del usuario en listas de distribución, foros, servicios de noticias, etc., que no sean consecuencia de la actividad profesional del usuario.

2. Quedan prohibidos aquellos usos del correo electrónico corporativo que puedan perjudicar la imagen de la Administración de la Comunidad Autónoma de Cantabria, sus representantes y empleados públicos, así como de los organismos públicos o privados con los que se mantiene relación, y en particular:

- a) El envío de correos electrónicos con contenido inadecuado, ilegal, ofensivo, difamatorio, inapropiado o discriminatorio por razón de sexo, raza, edad o discapacidad.
- b) El envío de mensajes o cartas en cadena y/o correos basura o spam (correo electrónico no solicitado).
- c) El envío de correos con programas informáticos (software) sin licencia, que vulneren los derechos de propiedad intelectual.
- d) El envío de correos de alerta de virus falsos.
- e) Realizar actividades de promoción de intereses personales.

3. Quedan prohibidos los accesos indebidos o suplantaciones del correo electrónico corporativo, y en particular:

- a) El acceso a un buzón de correo electrónico distinto del propio sin la correspondiente autorización.

CVE-2016-6831

- b) El envío de correos electrónicos con credenciales distintas a las asignadas legítimamente.
- c) Suplantar la identidad de un usuario interno de la organización o de Internet.
- 4. Queda prohibido el uso continuado y abusivo del correo electrónico corporativo con fines personales.

Artículo 13. Usos aceptables de la navegación web.

1. El acceso corporativo a la navegación en Internet, o a otros servicios de acceso a contenidos en Internet, es un recurso que la Administración de la Comunidad Autónoma de Cantabria pone a disposición de los usuarios, como herramienta necesaria para el acceso a contenidos y recursos de Internet necesarios para el desempeño de su actividad profesional.

2. Las conexiones que se realicen a Internet deben obedecer a fines profesionales, teniendo siempre en cuenta que se están utilizando recursos informáticos restringidos y escasos. El acceso a Internet para fines personales debe limitarse y de ser absolutamente necesario, sólo debe utilizarse un tiempo razonable, que no interfiera en el rendimiento profesional ni en la eficiencia de los recursos informáticos corporativos.

3. Sólo se podrá acceder a Internet mediante el navegador o navegadores suministrados y configurados en los equipos suministrados de usuario. No podrá alterarse la configuración del mismo ni utilizar un navegador alternativo, sin la debida autorización.

Artículo 14. Usos prohibidos de la navegación web.

1. Quedan prohibidos aquellos usos de la navegación web que puedan perjudicar al funcionamiento o a la seguridad de los sistemas tecnológicos o de información o a la información que contienen, y en particular:

a) El acceso a páginas web u otros servicios disponibles en Internet potencialmente peligrosos.

b) La descarga de programas informáticos o ficheros con contenido dañino que supongan una fuente de riesgos para la organización, sus sistemas o su información.

c) La descarga de archivos voluminosos o la descarga masiva de archivos, según los estándares de uso habituales, que pueda afectar al rendimiento de los sistemas y las redes.

2. Quedan prohibidos aquellos usos de la navegación web que puedan perjudicar la imagen de la Administración de la Comunidad Autónoma de Cantabria, sus representantes y empleados públicos, así como de los organismos públicos o privados con los que se mantiene relación, y en particular:

a) El acceso a otras redes, con el propósito de violar su integridad o seguridad.

b) La publicación o envío de mensajes a través de Internet que contengan amenazas, ofensas o imputación de hechos que puedan lesionar la dignidad personal.

c) La descarga de archivos que supongan la violación de la legislación de en materia de protección intelectual.

3. Quedan prohibido el acceso a contenidos no relacionados con las tareas encomendadas y puedan afectar al rendimiento profesional.

Artículo 15. Usos aceptables de las redes sociales, el almacenamiento en la nube y otros medios novedosos para la difusión o almacenamiento de información.

1. El uso desde equipos corporativos de las redes sociales, los sistemas de almacenamiento en la nube, u otros servicios futuros de similares características, debe evitarse salvo en aquellos casos en que esté directamente relacionado con las tareas profesionales encomendadas y en cualquier caso nunca debe afectar al desempeño profesional, ni al rendimiento de los recursos y sistemas, ni poner en peligro su seguridad o la de la información que contienen.

2. Los sistemas de almacenamiento en la nube, salvo aquellos que sean expresamente autorizados por la Administración de la Comunidad Autónoma de Cantabria, nunca deben emplear para el almacenamiento de información confidencial o reservada.

LUNES, 1 DE AGOSTO DE 2016 - BOC NÚM. 147

3. Ni las redes sociales ni los sistemas de almacenamiento en la nube deben usarse para ningún tipo de actividad ilícita.

Artículo 16. Usos aceptables de la telefonía y los sistemas de videoconferencia.

La utilización de los sistemas de telefonía o videoconferencia proporcionados por la Administración de la Comunidad Autónoma de Cantabria a sus usuarios tendrá una orientación profesional.

Artículo 17. Usos prohibidos de la telefonía y los sistemas de videoconferencia.

1. Queda prohibido manipular los sistemas de telefonía y videoconferencia para comprometer la seguridad, la estabilidad de las redes y sistemas o la confidencialidad de las comunicaciones.

2. Queda prohibido emplear los equipos de videoconferencia para visualizar personas o ubicaciones remotas sin su conocimiento.

3. Queda prohibido realizar campañas de promoción personal, de productos o cualquier uso que suponga un gasto no justificado.

4. Queda prohibido utilizar los sistemas y redes para cualquier finalidad delictiva o fraudulenta.

Artículo 18. Usos aceptables de los sistemas de teletrabajo.

1. El uso de los accesos remotos que permiten el teletrabajo estará destinado a la realización de las tareas profesionales encomendadas.

2. La concesión de credenciales para el uso de estos accesos remotos se hará de forma controlada, previa autorización y sólo para los casos en que esté justificado.

Artículo 19. Usos específicamente prohibidos de los sistemas de teletrabajo.

1. El acceso a los sistemas de teletrabajo utilizando conexiones inseguras o desconocidas.

2. Queda prohibido permitir a terceras personas visualizar o acceder de alguna manera a informaciones albergadas en los sistemas informáticos de la Administración de la Comunidad Autónoma de Cantabria, salvo autorización expresa.

3. Está prohibido utilizar la conexión remota para intentar comprometer de algún modo la seguridad de los sistemas tecnológicos y servicios informáticos de la Administración de la Comunidad Autónoma de Cantabria.

4. Queda prohibido hacer acciones que comprometan el buen funcionamiento de los sistemas de teletrabajo.

Artículo 20. Acceso a información.

Los usuarios sólo podrán acceder a aquella información para la que posean las debidas y explícitas autorizaciones, vinculadas a las tareas profesionales que tengan encomendadas en función de su puesto de trabajo, no pudiendo en ningún caso acceder a información perteneciente a otros usuarios o grupos de usuarios para los que no se posea tal autorización.

Artículo 21. Medidas de seguridad sobre la información.

1. Los usuarios deberán almacenar sus ficheros de trabajo en las carpetas de red que le hayan sido asignadas, sobre las que hay garantías de seguridad, incluida la realización de copias de seguridad.

2. Se evitará almacenar información privada, de cualquier naturaleza, en los recursos de almacenamiento compartido o local.

LUNES, 1 DE AGOSTO DE 2016 - BOC NÚM. 147

3. Se evitará dejar visible en la pantalla del ordenador información reservada o confidencial.

4. Se harán copias de seguridad periódicamente, para que la información pueda ser recuperada en caso de que se produzca algún incidente. Estas copias se harán automáticamente, sin la necesidad de que intervenga el usuario. Para recuperar esta información el usuario deberá realizar la correspondiente petición de servicio, que deberá ser aprobada por la persona con capacidad de decisión sobre esa información.

5. En el caso de que deban transmitirse información reservada o confidencial, se cifrará o se utilizará cualquier otro mecanismo que garantice que la información no será inteligible durante su remisión o transporte.

6. Sobre la información en papel o en otros soportes no tecnológicos:

a) Cuando se utilicen equipos de impresión o manipulación de documentos (faxes, impresoras, escáneres, etc.), se retirarán inmediatamente los documentos en papel, tanto los originales como sus copias de los equipos.

b) Si un usuario encuentra documentación confidencial o reservada en una fotocopiadora o impresora, intentará localizar a su propietario para que éste la recoja inmediatamente y si no es posible localizarlo notificará un incidente de seguridad.

c) Los documentos en papel que contengan información confidencial o reservada deben custodiarse bajo llave.

d) Cuando concluya la vida útil de los documentos impresos con información confidencial o reservada, deberán ser destruidos, de forma que no sea recuperable la información que pudieran contener.

Artículo 22. Confidencialidad sobre técnicas y metodologías.

Toda información de carácter confidencial o reservada que se conozca acerca de las técnicas y metodologías empleadas por la Administración de la Comunidad Autónoma de Cantabria en la ejecución de cualquier tarea no podrá ser comunicada a terceros ni emplearla en uso propio.

Artículo 23. Usos prohibidos de la información.

1. Queda prohibido acceder a información confidencial o reservada alojada en los recursos y sistemas tecnológicos y de información en la Administración de la Comunidad Autónoma de Cantabria sin la debida autorización.

2. Queda prohibido comunicar, divulgar, distribuir, publicar o poner en conocimiento o al alcance de terceros (externos o internos no autorizados), por cualquier medio (correo electrónico, web, redes sociales, etc.), información confidencial o reservada alojada en los sistemas tecnológicos o de información de la Administración de la Comunidad Autónoma de Cantabria, salvo que la actuación sea realizada en cumplimiento de las tareas profesionales encomendadas y esté debidamente autorizada.

3. Queda prohibido transmitir o alojar información confidencial o reservada propia de la Administración de la Comunidad Autónoma de Cantabria en servidores externos. En el caso de que se autorice, se comprobará la inexistencia de trabas legales para ello y se verificará la suscripción de un contrato expreso entre la Administración de la Comunidad Autónoma de Cantabria y la empresa responsable de la prestación del servicio, incluyendo los Acuerdos de Nivel de Servicio que procedan, el correspondiente Acuerdo de Confidencialidad, y siempre previo análisis de los riesgos asociados a tal externalización.

4. Queda prohibido utilizar la información para propósitos que puedan influir negativamente en la imagen de la Administración de la Comunidad Autónoma de Cantabria, de sus representantes y empleados públicos o de los organismos públicos o privados con los que se mantiene relación.

Artículo 24. Protección de datos de carácter personal.

1. La información de la Administración de la Comunidad Autónoma de Cantabria que comprenda datos de carácter personal está protegida por la Ley Orgánica 15/1999, de 13 de di-

CVE-2016-6831

ciembre, de Protección de Datos de Carácter Personal (LOPD) y su normativa derivada o de desarrollo.

2. Para garantizar dicha protección, se adoptarán las medidas de seguridad que se correspondan con las exigencias previstas en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

3. También se tendrán previstas las necesarias adaptaciones para el cumplimiento del Reglamento (UE) 2016/679 Del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

Artículo 25. Responsabilidades de los usuarios.

1. Los usuarios de los recursos y sistemas tecnológicos o de información de la Administración de la Comunidad Autónoma de Cantabria tienen las siguientes responsabilidades directas:

a) Utilizar los sistemas información, así como la información que contienen, para fines profesionales en el desarrollo de las tareas que tenga encomendadas, evitando cualquier uso personal que pueda afectar a la seguridad o al propio desempeño profesional.

b) Custodiar las credenciales que se le proporcionen, respetar las normas y seguir todas las recomendaciones de seguridad que elabore la Administración de la Comunidad Autónoma de Cantabria para garantizar que aquellas no puedan ser utilizadas por terceros.

c) En el caso de que su equipo permita el acceso a información confidencial o reservada, o bien utilice soportes que la almacenen, deberá cumplir todos los requisitos legales aplicables, así como las medidas de protección que la política de seguridad o las normas de seguridad establezcan.

2. Además, los usuarios no deberán acceder a los sistemas y recursos de la Administración de la Comunidad Autónoma de Cantabria para desarrollar actividades que persigan o tengan como consecuencia:

a) Dañar los recursos informáticos propios o ajenos.

b) El uso intensivo de recursos de proceso, memoria, almacenamiento o comunicaciones, para usos no profesionales.

c) La degradación de los servicios.

d) La destrucción o modificación no autorizada de la información, de manera premeditada.

e) La violación de la intimidad, del secreto de las comunicaciones y del derecho a la protección de los datos personales.

f) El deterioro intencionado del trabajo de otras personas.

g) Incurrir en cualquier otra actividad ilícita, del tipo que sea.

Artículo 26. Información para los usuarios.

1. El órgano directivo competente en materia informática pondrá en marcha los mecanismos necesarios para la difusión efectiva de las normas de seguridad contenidas en la presente orden entre los usuarios de los recursos y servicios tecnológicos y de información de la Administración de la Comunidad Autónoma de Cantabria.

2. Así mismo, la Administración de la Comunidad Autónoma de Cantabria podrá enviar información a los usuarios de sus recursos y sistemas tecnológicos o de información relativa a su utilización, su seguridad o también de otro tipo que se considere oportuno, empleando los medios que ha puesto a su disposición (correo electrónico, webs, sesiones de usuario, etc.).

Artículo 27. Incumplimiento de la normativa.

En el supuesto de que un usuario no respete alguna de las normas de seguridad incluidas en la presente orden, sin perjuicio de las acciones disciplinarias y administrativas que procedan

LUNES, 1 DE AGOSTO DE 2016 - BOC NÚM. 147

y, en su caso, las responsabilidades legales correspondientes, se podrá acordar la suspensión temporal o definitiva del uso de los recursos tecnológicos asignados a tal usuario.

Disposición final primera. Desarrollo de las normas de seguridad incluidas en esta orden.

1. Se faculta al Director General con competencias en materia informática para aprobar procedimientos de seguridad que desarrollen las normas de seguridad que se incluyen en la presente orden para conseguir su aplicación práctica y adaptarlas a la evolución de los recursos y sistemas tecnológicos y de información de la Administración de la Comunidad Autónoma de Cantabria.

2. También procurará que se pongan en marcha las medidas técnicas y operativas que sean oportunas.

Disposición final segunda. Entrada en vigor.

La presente orden entrará en vigor el día siguiente de su publicación en el Boletín Oficial de Cantabria.

Santander, 22 de julio de 2016.
El consejero de Presidencia y Justicia,
Rafael de la Sierra González.

[2016/6831](#)

CVE-2016-6831