

Conselleria d'Hisenda i Administració Pública

ORDE 19/2013, de 3 de desembre, de la Conselleria d'Hisenda i Administració Pública, per la qual s'establixen les normes sobre l'ús segur de mitjans tecnològics en l'Administració de la Generalitat. [2013/11767]

PREÀMBUL

La informació constituïx un actiu de primer orde per a la Generalitat des del moment que resulta essencial per a la prestació de gran part dels seus servicis. D'altra banda, les tecnologies de la informació i les comunicacions s'han fet cada vegada més imprescindibles per a les administracions públiques. No obstant això, les indiscutibles millores que aporten al tractament de la informació van acompanyades de nous riscos i, per tant, és necessari introduir mesures específiques per a protegir tant la informació com els servicis que en depenguen.

La seguretat de la informació té com a objectiu protegir la informació tractada i els servicis que es presten, reduint els riscos a què estan sotmesos fins a un nivell que resulte acceptable. Dins de cada organització només els seus màxims directius tenen les competències necessàries per a fixar este nivell, ordenar les actuacions i habilitar els mitjans per a dur-les a terme.

En aplicació del Reial Decret 3/2010, pel qual es regula l'Esquema Nacional de Seguretat en l'àmbit de l'Administració electrònica, l'Administració de la Generalitat i de les seues entitats autònomes han de protegir la informació i els servicis utilitzats en mitjans electrònics que gestionen en l'exercici de les seues competències. Per a això han d'assegurar la integritat, la disponibilitat, l'autenticitat, la confidencialitat, la traçabilitat i la conservació de les dades, les informacions i els servicis utilitzats en els mitjans tecnològics que gestionen en l'exercici de les seues competències.

El Decret 66/2012, de 27 d'abril, del Consell, pel qual s'establix la política de seguretat de la informació de la Generalitat en l'àmbit de l'Administració de la Generalitat i de les seues entitats autònomes, indica que la política es desenrotllarà en un conjunt de documents l'objectiu dels quals és facilitar que el tractament d'informació es realitze d'acord amb els objectius i principis que s'hi exposen, i que estos s'agruparan en tres col·leccions: normes, procediments i guies de bones pràctiques. Les normes proporcionaran un primer nivell de concreció; cada una estarà dirigida a un tipus d'activitat determinat. Els procediments descriuran la seqüència concreta de passos per a completar una tasca. Les guies de bones pràctiques oferiran recomanacions sobre com actuar en situacions específiques. Les normes i els procediments tindran caràcter obligatori.

L'objecte d'esta disposició és regular la norma d'ús segur dels mitjans tecnològics que formen part dels sistemes d'informació de l'Administració de la Generalitat, a fi de minimitzar la probabilitat de la materialització de les amenaces que posen en risc la seguretat dels sistemes d'informació.

El Decret 130/2012, de 24 d'agost, del Consell, pel qual s'establix l'organització de la seguretat de la informació de la Generalitat, assigna el repartiment de funcions i responsabilitats en matèria de seguretat de la informació aplicable a les conselleries de la Generalitat, així com a les seues entitats autònomes dependents.

L'Orde 9/2012, de 10 de juliol, de la Conselleria de Sanitat, per la qual s'establix l'organització de la seguretat de la informació, fa un repartiment efectiu de tasques i responsabilitats per al manteniment i la millora de la seguretat de la informació en la Conselleria de Sanitat.

Per això, i en virtut de les facultats que em conferix l'article 28 de la Llei 5/1983, de 30 de desembre, del Consell, i la disposició final primera del Decret 66/2012, de 27 d'abril, del Consell, pel qual s'establix la política de seguretat de la informació de la Generalitat,

ORDENE

CAPÍTOL I

Disposicions preliminars

Article 1. Objecte

Esta orde té per objecte regular la norma d'ús segur dels mitjans tecnològics que formen part dels sistemes d'informació de l'Adminis-

Consellería de Hacienda y Administración Pública

ORDEN 19/2013, de 3 de diciembre, de la Consellería de Hacienda y Administración Pública, por la que se establecen las normas sobre el uso seguro de medios tecnológicos en la Administración de la Generalitat. [2013/11767]

PREÁMBULO

La información constituye un activo de primer orden para la Generalitat desde el momento en que resulta esencial para la prestación de gran parte de sus servicios. Por otro lado las tecnologías de la información y las comunicaciones se han hecho cada vez más imprescindibles para las administraciones públicas. Sin embargo, las indiscutibles mejoras que aportan al tratamiento de la información vienen acompañadas de nuevos riesgos, y por lo tanto es necesario introducir medidas específicas para proteger tanto la información como los servicios que dependan de ella.

La seguridad de la información tiene como objetivo proteger la información tratada y los servicios que se prestan, reduciendo los riesgos a los que están sometidos hasta un nivel que resulte aceptable. Dentro de cada organización solo sus máximos directivos tienen las competencias necesarias para fijar dicho nivel, ordenar las actuaciones y habilitar los medios para llevarlas a cabo.

En aplicación del Real Decreto 3/2010, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, la Administración de la Generalitat y de sus entidades autónomas deben proteger la información y los servicios utilizados en medios electrónicos que gestionen en el ejercicio de sus competencias. Para ello deben asegurar la integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en los medios tecnológicos que gestionen en el ejercicio de sus competencias.

El Decreto 66/2012, de 27 de abril, del Consell, por el que se establece la política de seguridad de la información de la Generalitat, en el ámbito de la Administración de la Generalitat y de sus entidades autónomas, indica que la política se desarrollará en un conjunto de documentos cuyo objetivo es facilitar que el tratamiento de información se realice de acuerdo con los objetivos y principios expuestos en la misma; y que estos se agruparán en tres colecciones: normas, procedimientos y guías de buenas prácticas. Las normas proporcionarán un primer nivel de concreción; cada una de ellas estará dirigida a un tipo de actividad determinado. Los procedimientos describirán la secuencia concreta de pasos para completar una tarea. Las guías de buenas prácticas ofrecerán recomendaciones sobre cómo actuar en situaciones específicas. Las normas y procedimientos tendrán carácter obligatorio.

El objeto de la presente disposición es regular la norma de uso seguro de los medios tecnológicos que forman parte de los sistemas de información de la Administración de la Generalitat, con el fin de minimizar la probabilidad de la materialización de las amenazas que ponen en riesgo la seguridad de los sistemas de información.

El Decreto 130/2012, de 24 de agosto, del Consell, por el que se establece la organización de la seguridad de la información de la Generalitat, asigna el reparto de funciones y responsabilidades en materia de seguridad de la información, aplicable a las consellerías de la Generalitat, así como a sus entidades autónomas dependientes.

La Orden 9/2012, de 10 de julio, de la Consellería de Sanidad, por la que establece la organización de la seguridad de la información, hace un reparto efectivo de tareas y responsabilidades para el mantenimiento y mejora de la seguridad de la información en la Consellería de Sanidad.

Por ello, y en virtud de las facultades que me confiere el artículo 28 de la Ley 5/1983, de 30 de diciembre, del Consell y la Disposición Final Primera del Decreto 66/2012, de 27 de abril, del Consell, por el que se establece la política de seguridad de la información de la Generalitat,

ORDENO

CAPÍTULO I

Disposiciones preliminares

Artículo 1. Objeto

La presente orden tiene por objeto regular la norma de uso seguro de los medios tecnológicos que forman parte de los sistemas de infor-

tració de la Generalitat, a fi de minimitzar la probabilitat de la materialització de les amenaces que posen en risc la seguretat dels sistemes d'informació.

Article 2. Àmbit d'aplicació

1. En l'àmbit d'esta normativa, s'entén per usuari qualsevol persona que utilitze o posseísca accés als mitjans tecnològics posats a la seua disposició per l'Administració de la Generalitat.

2. Les normes enunciades en esta orde seran de compliment obligatori per a tots els usuaris definits en el punt anterior.

3. Els seus continguts desenrotllen les directrius de caràcter general definides en la política de seguretat de la informació, tenint en compte que es podran definir normes restrictives en certs àmbits específics que ho requerisquen.

Article 3. Principi general d'actuació

La seguretat de la informació depén de totes les persones que participen en el seu tractament i comprometen a totes les que integren l'organització. Tots els usuaris es comprometen a fer un ús correcte de tots els actius que requerisquen per al desenrotllament de les seues funcions, a respectar les mesures de seguretat que s'establisquen i a notificar com més prompte millor als responsables que corresponga els esdeveniments i punts dèbils de la seguretat de la informació que detecten, de manera que puguen emprendre's les accions oportunes.

Article 4. Definicions

Als efectes previstos en esta orde, les definicions, paraules, expressions i termes han de ser entesos en el sentit indicat en la normativa de protecció de dades de caràcter personal, en l'esquema nacional de seguretat i en el glossari inclòs en l'annex.

CAPÍTOL II *Normes generals*

Article 5. Tractament de la informació

1. L'Administració de la Generalitat serà responsable del tractament de la informació en qualsevol mitjà tecnològic que forme part dels seus sistemes d'informació i xarxes de comunicacions, i adoptarà les mesures d'índole tècnica i organitzatives necessàries que garantisquen la seguretat de les dades.

2. Els qui per raó de l'exercici de les seues funcions accedisquen a informació que no siga d'accés públic hauran d'observar la necessària reserva, confidencialitat i sigil, inclús després d'haver cessat en les seues funcions o finalitzat la relació contractual o laboral.

3. Els qui tracten informació que no haja sigut classificada d'accés públic hauran d'estar degudament identificats i tindre els privilegis d'accés a la informació estrictament imprescindibles per a exercir la seua comesa.

4. Queda prohibit, així mateix, transmetre o allotjar informació pròpia de l'Administració de la Generalitat en sistemes d'informació externs, excepte autorització expressa de l'organisme responsable del tractament de la informació, que comprovarà la inexistència de traves legals per a això i verificarà la subscripció d'un contracte exprés entre l'Administració de la Generalitat i l'empresa responsable de la prestació del servei, incloent-hi els acords de nivell de servei que siguen procedents, l'acord de confidencialitat corresponent i sempre amb l'anàlisi prèvia dels riscos associats a tal externalització.

Article 6. Propietat i ús dels mitjans tecnològics

1. Tots els mitjans tecnològics posats a disposició dels usuaris: ordinadors personals i portàtils, aplicacions, programes, sistemes d'impressió i escaneig de documents, dispositius mòbils, l'accés a la xarxa corporativa i a Internet són propietat de l'Administració de la Generalitat.

2. L'Administració de la Generalitat proporcionarà a cada usuari un lloc de treball amb els mitjans tecnològics necessaris per a l'exercici de les funcions encomanades.

3. Estos mitjans no estan destinats a l'ús personal, i no podran utilitzar-se per a activitats il·lícites o irregulars, o que afecten negativament el funcionament de l'Administració de la Generalitat o siguen contràries als interessos d'esta.

mación de la Administración de la Generalitat, con el fin de minimizar la probabilidad de la materialización de las amenazas que ponen en riesgo la seguridad de los sistemas de información.

Artículo 2. Ámbito de aplicación

1. En el ámbito de la presente normativa, se entiende por usuario a cualquier persona que utilice o posea acceso a los medios tecnológicos puestos a su disposición por la Administración de la Generalitat.

2. Las normas enunciadas en la presente orden serán de obligado cumplimiento para todos los usuarios definidos en el punto anterior.

3. Sus contenidos desarrollan las directrices de carácter general definidas en la política de seguridad de la información, teniendo en cuenta que se podrán definir normas restrictivas en ciertos ámbitos específicos que lo precisen.

Artículo 3. Principio general de actuación

La seguridad de la información depende de todas las personas que participan en su tratamiento y compromete a todas las que integran la organización. Todos los usuarios se comprometen a hacer un uso correcto de todos los activos que requieran para el desarrollo de sus funciones, a respetar las medidas de seguridad que se establezcan y a notificar lo antes posible a los responsables que corresponda de los eventos y puntos débiles de la seguridad de la información que detecten, de manera que puedan emprenderse las acciones oportunas.

Artículo 4. Definiciones

A los efectos previstos en esta orden, las definiciones, palabras, expresiones, y términos han de ser entendidos en el sentido indicado en la normativa de protección de datos de carácter personal, en el esquema nacional de seguridad y en el glosario incluido en el Anexo.

CAPÍTULO II *Normas generales*

Artículo 5. Tratamiento de la información

1. La Administración de la Generalitat será responsable del tratamiento de la información en cualquier medio tecnológico que forme parte de sus sistemas de información y redes de comunicaciones, y adoptará las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos.

2. Quienes por razón del ejercicio de sus funciones accedan a información que no sea de acceso público, deberán observar la necesaria reserva, confidencialidad y sigilo, incluso después de haber cesado en sus funciones o finalizado la relación contractual o laboral.

3. Quienes traten información que no haya sido clasificada de acceso público, deberán estar debidamente identificados y tener los privilegios de acceso a la información estrictamente imprescindibles para desempeñar su cometido.

4. Queda prohibido, asimismo, transmitir o alojar información propia de la Administración de la Generalitat en sistemas de información externos, salvo autorización expresa del organismo responsable del tratamiento de la información, que comprovará la inexistencia de trabas legales para ello y verificará la suscripción de un contrato expreso entre la Administración de la Generalitat 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.

Artículo 6. Propiedad y uso de los medios tecnológicos

1. Todos los medios tecnológicos puestos a disposición de los usuarios: ordenadores personales y portátiles, aplicaciones, programas, sistemas de impresión y escaneo de documentos, dispositivos móviles, el acceso a la red corporativa y a internet, son propiedad de la Administración de la Generalitat.

2. La Administración de la Generalitat le proporcionará a cada usuario un puesto de trabajo con los medios tecnológicos necesarios para el desempeño de las funciones encomendadas.

3. Dichos medios no están destinados al uso personal, y no podrán utilizarse para actividades ilícitas o irregulares, o que afecten negativamente al funcionamiento de la Administración de la Generalitat o sean contrarias a los intereses de esta.

4. Està prohibit alterar, sense la deguda autorització, qualsevol dels components físics o lògics dels mitjans tecnològics, excepte autorització expressa de l'organisme amb competències en tecnologies de la informació. En tot cas, estes operacions només podran realitzar-se pel personal de suport tècnic autoritzat.

5. La instal·lació, utilització o connexió a la xarxa corporativa de qualsevol mitjà tecnològic alié requerirà una autorització prèvia per part de l'òrgan competent en matèria de tecnologies de la informació que corresponga.

6. Està estrictament prohibida l'execució de programes informàtics en els mitjans tecnològics que formen part dels sistemes d'informació de l'Administració de la Generalitat sense la llicència d'ús i autorització corresponents de l'organisme amb competències en tecnologies de la informació.

7. Està terminantment prohibida tota transmissió, distribució o emmagatzematge de qualsevol material obscé, difamatori, amenaçador o que constituïska un atemptat contra la dignitat de les persones.

Article 7. Identificació d'accés

1. La identificació d'accés a qualsevol mitjà tecnològic serà personal i intransferible, i permetrà una identificació individual.

2. Els usuaris han de custodiar convenientment la seua identificació d'accés, són responsables de tota l'activitat relacionada amb l'ús del seu accés personal autoritzat i en cap cas podrà ser subministrada a terceres persones.

3. Si un usuari té sospites que la seua identificació d'accés està sent utilitzada per una altra persona, haurà de comunicar immediatament a l'organisme amb competències en tecnologies de la informació la incidència de seguretat corresponent.

4. Els usuaris han d'utilitzar contrasenyes segures d'acord amb la política de contrasenyes definida per l'òrgan amb competències en matèria de tecnologies de la informació.

Article 8. Notificació d'incidències

1. Constituïx una incidència de seguretat en un sistema qualsevol situació o eventualitat en què puga veure's amenaçada la informació i puga, en conseqüència, donar lloc a una pèrdua de confidencialitat, integritat, disponibilitat i autenticitat.

2. Tots els usuaris estan obligats a notificar qualsevol incidència de seguretat a través del procediment establert a este efecte.

Article 9. Implantació de mesures tècniques

El personal que realitza funcions en matèria de tecnologies de la informació adoptarà les mesures tècniques adequades al nivell de seguretat establert per a cada tractament de la informació i en la prestació dels servicis, pel responsable designat en l'organització de la seguretat.

Article 10. Esborrament i destrucció de suports d'informació

1. Es destruiran de forma segura els suports d'informació que hagen de ser rebutjats.

2. Els suports d'informació que hagen de ser reutilitzats per a una altra informació o lliurats a una altra organització seran objecte d'un esborrament segur del seu contingut anterior.

Article 11. Inspecció dels mitjans tecnològics

L'òrgan competent en matèria de tecnologies de la informació establirà, per raons específiques de seguretat o d'avaluació de l'exercici, mesures de control i comprovarà, per mitjà dels mecanismes formals i tècnics que crega oportuns, la utilització correcta per part dels usuaris de tots els mitjans tecnològics posats a la seua disposició per a l'exercici de les seues funcions. Estos controls i revisions es realitzaran respectant els principis de necessitat, idoneïtat i proporcionalitat, preservant les garanties del dret a la intimitat de l'usuari i la seguretat de les comunicacions.

Article 12. Cessament d'activitat

1. El cessament d'activitat de qualsevol usuari ha de ser comunicat de forma immediata a l'organisme amb competències en tecnologies de la informació.

4. Está prohibido alterar, sin la debida autorización, cualquiera de los componentes físicos o lógicos de los medios tecnológicos, salvo autorización expresa del organismo con competencias en tecnologías de la información. En todo caso, estas operaciones solo podrán realizarse por el personal de soporte técnico autorizado.

5. La instalación, utilización o conexión a la red corporativa de cualquier medio tecnológico ajeno, requerirá una autorización previa por parte del órgano competente en materia de tecnologías de la información que corresponda.

6. Está estrictamente prohibida la ejecución de programas informáticos en los medios tecnológicos que forman parte de los sistemas de información de la Administración de la Generalitat sin la correspondiente licencia de uso y autorización correspondiente del organismo con competencias en tecnologías de la información.

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

Artículo 7. Identificación de acceso

1. La identificación de acceso a cualquier medio tecnológico será personal e intransferible, permitiendo una identificación individual.

2. Los usuarios deben custodiar convenientemente su identificación de acceso, son responsables de toda la actividad relacionada con el uso de su acceso personal autorizado, y en ningún caso podrá ser suministrada a terceras personas.

3. Si un usuario tiene sospechas de que su identificación de acceso está siendo utilizada por otra persona, deberá comunicar inmediatamente al organismo con competencias en tecnologías de la información la correspondiente incidencia de seguridad.

4. Los usuarios deben utilizar contraseñas seguras de acuerdo con la política de contraseñas definida por el órgano con competencias en materia de tecnologías de la información.

Artículo 8. Notificación de incidencias

1. Una incidencia de seguridad en un sistema, la constituye cualquier situación o eventualidad en la que pueda verse amenazada la información, y pueda en consecuencia dar lugar a una pérdida de: confidencialidad, integridad, disponibilidad y autenticidad.

2. Todos los usuarios están obligados a notificar cualquier incidencia de seguridad a través del procedimiento establecido a tal efecto.

Artículo 9. Implantación de medidas técnicas

El personal que realiza funciones en materia de tecnologías de la información, adoptará las medidas técnicas adecuadas al nivel de seguridad establecido para cada tratamiento de la información y en la prestación de los servicios, por el responsable designado en la organización de la seguridad.

Artículo 10. Borrado y destrucción de soportes de información

1. Se destruirán de forma segura los soportes de información que vayan a ser desechados.

2. Los soportes de información que vayan a ser reutilizados para otra información o liberados a otra organización serán objeto de un borrado seguro de su anterior contenido.

Artículo 11. Inspección de los medios tecnológicos

El órgano competente en materia de tecnologías de la información establecerá por razones específicas de seguridad o de evaluación del desempeño, medidas de control y comprobará mediante los mecanismos formales y técnicos que estime oportunos, la correcta utilización por parte de los usuarios de todos los medios tecnológicos 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.

Artículo 12. Cese de actividad

1. El cese de actividad de cualquier usuario debe ser comunicado de forma inmediata al organismo con competencias en tecnologías de la información.

2. Quan es modifiquen les circumstàncies professionals que van originar l'entrega d'un mitjà tecnològic, l'usuari el tornarà a l'organisme amb competències en tecnologies de la informació, a fi de procedir a l'esborrament segur de la informació emmagatzemada i restaurar l'equip al seu estat original perquè pugui ser assignat a un nou usuari.

Article 13. Còpies de seguretat

La còpia de seguretat periòdica de les dades allotjades en els servidors corporatius és responsabilitat de l'òrgan competent en matèria de tecnologies de la informació. Cada usuari serà responsable de la integritat i còpia de seguretat de la informació emmagatzemada en el mitjà tecnològic que tinga assignat.

Article 14. Accés des de l'exterior

només està permès accedir des de l'exterior de la XCGVA (Xarxa Corporativa de la Generalitat Valenciana) a recursos interns quan se segueisca el procediment aprovat a este efecte per l'òrgan amb competències en matèria de tecnologies de la informació.

Article 15. Incumpliments

L'incumpliment de les normes d'ús expressades en esta orde podrà tindre conseqüències disciplinàries d'acord amb el règim sancionador aplicable en cada cas, sense perjudi d'altres responsabilitats en què es pugui incurrir.

CAPÍTOL III *Mitjans tecnològics*

Article 16. Ordinadors personals de sobretaula

1. No està permès alterar la configuració del maquinari dels equips ni connectar altres dispositius a estos a iniciativa de l'usuari, així com variar la seua ubicació.

2. No està permès alterar la configuració del programari dels equips, desinstal·lar o instal·lar programes diferents de la configuració establida per l'organisme amb competències en tecnologies de la informació.

3. És obligatori bloquejar la sessió de l'usuari en el supòsit d'absentarse temporalment del lloc de treball, a fi d'evitar accessos d'altres persones a l'equip informàtic. Així mateix, és obligatori apagar l'equip en acabar la jornada laboral.

4. L'emmagatzematge de fitxers generats en l'exercici de les competències professionals de l'usuari s'efectuarà en la carpeta habilitada en la xarxa informàtica, a fi de facilitar la realització de còpies de seguretat o suport i protegir l'accés davant de persones no autoritzades.

5. No està permès emmagatzemar informació privada, de qualsevol naturalesa, en els recursos d'emmagatzematge compartits.

6. No està permès copiar, extraure o transmetre informació continguda en el sistema informàtic per a ús privat o per a qualsevol altre diferent del servei públic a què està destinada.

7. Els fitxers temporals han de ser esborrats una vegada que hagen deixat de ser necessaris per als fins que van motivar la seua creació i, mentres estiguen vigents, hauran de ser emmagatzemats en la carpeta habilitada en la xarxa informàtica.

Article 17. Equips portàtils

1. Totes les responsabilitats aplicables als ordinadors de sobretaula són aplicables als equips portàtils.

2. Responsabilitats addicionals específiques dels equips portàtils:

a) Amb caràcter general, no s'emmagatzemarà informació sensible o confidencial en este tipus d'equips i, en cas de ser necessari, haurà de ser protegida per mitjà de ferramentes d'criptació.

b) Este tipus de dispositius estarà sota la custòdia de l'usuari que els utilitze. No es deixarà l'equip portàtil desatès o abandonat en llocs on pugui ser sostret amb facilitat.

c) Els usuaris d'estos equips es responsabilitzaran que no seran usats per usuaris no autoritzats.

2. Cuando se modifiquen las circunstancias profesionales que originaron la entrega de un medio tecnológico, el usuario lo devolverá al organismo con competencias en tecnologías de la información, al objeto de proceder al borrado seguro de la información almacenada y restaurar el equipo a su estado original para que pueda ser asignado a un nuevo usuario.

Artículo 13. Copias de seguridad

La copia de seguridad periódica de los datos alojados en los servidores corporativos es responsabilidad del órgano competente en materia de tecnologías de la información. Cada usuario será responsable de la integridad y copia de seguridad de la información almacenada en el medio tecnológico que tenga asignado.

Artículo 14. Acceso desde el exterior

Sólo está permitido acceder desde el exterior de la RCGVA (Red Corporativa de la Generalitat Valenciana) a recursos internos cuando se siga el procedimiento aprobado a tal efecto por el órgano con competencias en materia de tecnologías de la información.

Artículo 15. Incumplimientos

El incumplimiento de las normas de uso expresadas en esta orden podrá tener consecuencias disciplinarias, de acuerdo con el régimen sancionador aplicable en cada caso, sin perjuicio de otras responsabilidades en que se pudiera incurrir.

CAPÍTULO III *Medios tecnológicos*

Artículo 16. Ordenadores personales de sobremesa

1. No está permitido alterar la configuración hardware de los equipos ni conectar otros dispositivos a estos a iniciativa del usuario, así como variar su ubicación.

2. No está permitido alterar la configuración software de los equipos, desinstalar o instalar programas distintos a la configuración establecida por el organismo con competencias en tecnologías de la información.

3. Es obligatorio bloquear la sesión del usuario en el supuesto de ausentarse temporalmente del puesto de trabajo, a fin de evitar accesos de otras personas al equipo informático. Asimismo, es obligatorio apagar el equipo al terminar la jornada laboral.

4. El almacenamiento de ficheros generados en el desempeño de las competencias profesionales del usuario, se efectuará en la carpeta habilitada en la red informática, a fin de facilitar la realización de copias de seguridad o respaldo y proteger el acceso frente a personas no autorizadas.

5. No está permitido almacenar información privada, de cualquier naturaleza, en los recursos de almacenamiento compartidos.

6. No está permitido copiar, extraer o transmitir información contenida en el sistema informático para uso privado o para cualquier otro distinto del servicio público al que está destinada.

7. Los ficheros temporales deben ser borrados una vez hayan dejado de ser necesarios para los fines que motivaron su creación y, mientras estén vigentes, deberán ser almacenados en la carpeta habilitada en la red informática.

Artículo 17. Equipos portátiles

1. Todas las responsabilidades aplicables a los ordenadores de sobremesa son de aplicación para los equipos portátiles.

2. Responsabilidades adicionales específicas de los equipos portátiles:

a) Con carácter general, no se almacenará información sensible o confidencial en este tipo de equipos, y en caso de ser necesario, deberá ser protegida mediante herramientas de cifrado.

b) Este tipo de dispositivos estará bajo la custodia del usuario que los utilice. No se dejará el equipo portátil desatendido o abandonado en lugares donde pueda ser sustraído con facilidad.

c) Los usuarios de estos equipos se responsabilizarán de que no serán usados por usuarios no autorizados.

d) La pèrdua o robatori de qualsevol dispositiu o equip portàtil haurà de notificar-se immediatament a l'organisme amb competències en tecnologies de la informació.

e) No hauran de connectar-se directament a xarxes alienes.

f) Haurà d'estar desactivada la busca de xarxes sense fil.

3. Els usuaris d'equips portàtils hauran de realitzar connexions periòdiques almenys mensuals a la xarxa corporativa, segons les instruccions proporcionades per l'organisme amb competències en tecnologies de la informació, per a permetre l'actualització d'aplicacions, sistema operatiu, firmes d'antivirus i la resta de mesures de seguretat.

4. Sobre els ordinadors portàtils s'adoptaran les mesures tècniques adequades al nivell de seguretat establert atenent el tractament de la informació que haja d'efectuar.

Article 18. Impressores, fotocopiadores, escàners, faxos i equips multifunció

1. És obligatori l'ús de bústies d'impressió amb clau d'accés en els dispositius multifunció compartits que ho permeten.

2. Quan s'imprimisca documentació, esta haurà de romandre el menor temps possible en les safates d'eixida de les impressores, per a evitar que terceres persones hi puguen accedir.

3. S'hauran d'arreglar els originals de la fotocopiadora, impressora, escàner o equips multifunció una vegada finalitzat el procés de còpia o digitalització.

Article 19. Dispositius mòbils

1. Totes les responsabilitats d'ús específiques dels equips portàtils també ho són per als dispositius mòbils.

2. És obligatori configurar el dispositiu mòbil perquè passat un temps d'inactivitat passe automàticament a manera de suspensió i s'active el bloqueig de la pantalla.

Article 20. Dispositius d'emmagatzematge removibles autoritzats

1. Els dispositius d'emmagatzematge removibles autoritzats seran els proporcionats per l'Administració de la Generalitat, seran conformes a les normes de seguretat de l'organització i seran destinats a un ús exclusivament professional, com a ferramenta de transport de fitxers, i no com a ferramenta d'emmagatzematge.

2. En cas de ser necessari emmagatzemar informació sensible o confidencial en este tipus de dispositiu, haurà de ser protegida per mitjà de ferramentes d'criptació.

3. Este tipus de dispositius estarà sota la custòdia de l'usuari que els utilitze. No es deixarà el dispositiu desatès o abandonat en llocs on puga ser sostret amb facilitat.

4. La pèrdua o robatori de qualsevol dispositiu d'emmagatzematge removable haurà de notificar-se immediatament a l'organisme amb competències en tecnologies de la informació.

Article 21. Correu electrònic corporatiu

1. Els comptes creats en els servidors de l'Administració de la Generalitat tenen com a objectiu l'intercanvi de missatges propis de l'exercici professional. Queda prohibit el seu ús amb fins comercials, financers o personals.

2. No estan permesos els enviaments massius, i seran rebutjats els missatges si el nombre màxim de destinataris és superior al límit establert per l'òrgan amb competències en matèria de tecnologies de la informació.

3. No s'ha d'utilitzar el correu per a anunciar l'aparició de nous virus, amenaces, etc.

4. Queda totalment prohibit suplantar la identitat d'una persona a través del correu electrònic.

5. No es permet l'ús de comptes de correu diferents dels proporcionats per l'Administració de la Generalitat dins de la XCGVA, excepte autorització expressa de l'òrgan amb competències en matèria de tecnologies de la informació.

6. Els usuaris no han d'enviar missatges amb informació sensible tant en el cos del missatge com en els arxius adjunts. Este enviament únicament podrà realitzar-se si s'adopten els mecanismes necessaris per a evitar que la informació siga intel·ligible o manipulada per tercers (criptació i firma electrònica).

d) La pèrdua o robo de cualquier dispositivo o equipo portátil deberá notificarse de inmediato al organismo con competencias en tecnologías de la información.

e) No deberán conectarse directamente a redes ajenas.

f) Deberá estar desactivada la búsqueda de redes inalámbricas.

3. Los usuarios de equipos portátiles deberán realizar conexiones periódicas al menos mensuales a la red corporativa, según las instrucciones proporcionadas por el organismo con competencias en tecnologías de la información, para permitir la actualización de aplicaciones, sistema operativo, firmas de antivirus y demás medidas de seguridad.

4. Sobre los ordenadores portátiles se adoptarán las medidas técnicas adecuadas al nivel de seguridad establecido atendiendo al tratamiento de la información que vaya a efectuar.

Artículo 18. Impresoras, fotocopiadoras, escáneres, faxes y equipos multifunción

1. Es obligatorio el uso de buzones de impresión con clave de acceso, en los dispositivos multifunción compartidos que lo permitan.

2. Cuando se imprima documentación, esta deberá permanecer el menor tiempo posible en las bandejas de salida de las impresoras, para evitar que terceras personas puedan acceder a la misma.

3. Se deberán recoger los originales de la fotocopiadora, impresora, escáner o equipos multifunción una vez finalizado el proceso de copia o digitalización.

Artículo 19. Dispositivos móviles

1. Todas las responsabilidades de uso específicas de los equipos portátiles, también lo son para los dispositivos móviles.

2. Es obligatorio configurar el dispositivo móvil para que pasado un tiempo de inactividad pase automáticamente a modo de suspensión y se active el bloqueo de la pantalla.

Artículo 20. Dispositivos de almacenamiento removibles autorizados

1. Los dispositivos de almacenamiento removibles autorizados serán los proporcionados por la Administración de la Generalitat, serán conformes a las normas de seguridad de la organización, y serán destinados a un uso exclusivamente profesional, como herramienta de transporte de ficheros, y no como herramienta de almacenamiento.

2. En caso de ser necesario almacenar información sensible o confidencial en este tipo de dispositivo, deberá ser protegida mediante herramientas de cifrado.

3. Este tipo de dispositivos estará bajo la custodia del usuario que los utilice. No se dejará el dispositivo desatendido o abandonado en lugares donde pueda ser sustraído con facilidad.

4. La pérdida o robo de cualquier dispositivo de almacenamiento removable deberá notificarse de inmediato al organismo con competencias en tecnologías de la información.

Artículo 21. Correo electrónico corporativo

1. Las cuentas creadas en los servidores de la Administración de la Generalitat tienen como objetivo el intercambio de mensajes propios del desempeño profesional. Queda prohibido su uso con fines comerciales, financieros o personales.

2. No están permitidos los envíos masivos, siendo rechazados los mensajes si el número máximo de destinatarios es superior al límite establecido por el órgano con competencias en materia de tecnologías de la información.

3. No se debe utilizar el correo para anunciar la aparición de nuevos virus, amenazas, etc.

4. Queda totalmente prohibido suplantar la identidad de una persona a través del correo electrónico.

5. No se permite el uso de cuentas de correo distintas a las proporcionadas por la Administración de la Generalitat dentro de la RCGVA, salvo autorización expresa del órgano con competencias en materia de tecnologías de la Información.

6. Los usuarios no deben enviar mensajes con información sensible tanto en el cuerpo del mensaje como en los archivos adjuntos. Este envío únicamente podrá realizarse si se adoptan los mecanismos necesarios para evitar que la información sea inteligible o manipulada por terceros (cifrado y firma electrónica).

7. El correu electrònic és una de les fonts més importants de difusió de virus, per la qual cosa es recomana no obrir missatges rebuts de remittents desconeguts.

8. Per a garantir la identitat del remitent, els correus es firmaran digitalment.

9. A causa de l'increment i la contínua aparició de nous virus, són eliminats automàticament els missatges amb annexos susceptibles d'execució.

10. Es limitarà la grandària màxima dels fitxers adjunts i s'assignarà als usuaris una grandària màxima de bústia, dins d'uns límits raonables.

Article 22. Accés a Internet des de la XCGVA

1. Condicions d'accés a Internet.

a) L'accés a Internet es realitzarà únicament a través de l'eixida a Internet establida per l'òrgan amb competències en matèria de tecnologies de la informació utilitzant els mitjans tecnològics que es disposen amb este fi.

b) L'accés a Internet per altres mitjans està expressament prohibit.

c) Els recursos d'Internet seran filtrats segons el seu contingut a través de sistemes automatitzats i cada usuari tindrà assignat un perfil d'accés en funció del seu lloc de treball, que determinarà a quin tipus de continguts podrà accedir i en quins horaris.

d) Els perfils d'accés seran creats per l'òrgan amb competències en matèria de tecnologies de la informació.

2. Responsabilitat de l'usuari final

a) La utilització d'Internet ha de limitar-se a l'obtenció d'informació relacionada amb el treball que s'exercix i, per tant, s'ha evitar-se tota utilització que no tinga una mínima relació amb les funcions encomanades a l'usuari o que pugua conduir a una millora de la qualitat del treball desenrotllat.

b) No està permès l'accés a pàgines de contingut ofensiu, inapropiat, pornogràfic o discriminatori per raons de gènere, ètnia, opció sexual, discapacitat o qualsevol altra circumstància personal o social.

c) No es permet la descàrrega des d'Internet de qualsevol classe de programes, aplicacions, documents o arxius que no provinguen de pàgines oficials relacionades amb el treball, tot això amb la finalitat que la descàrrega no pugua posar en perill els sistemes informàtics i la informació que la Generalitat custodia.

DISPOSICIONS FINALS

Primera. Desplegament

S'autoritza el centre superior o directiu amb competències en matèria de tecnologies de la informació a dictar les instruccions i ordes de servici, així com a adoptar les mesures que considere oportunes per al desplegament i l'aplicació d'esta orde.

Segona. Entrada en vigor

Esta orde entrarà en vigor l'endemà de la seua publicació en el *Diari Oficial de la Comunitat Valenciana*.

València, 3 de desembre de 2013

El conseller d'Hisenda i Administració Pública,
JUAN CARLOS MORAGUES FERRER

7. El correo electrónico es una de las fuentes más importantes de difusión de virus, por lo que se recomienda no abrir mensajes recibidos de remitentes desconocidos.

8. Para garantizar la identidad del remitente los correos se firmarán digitalmente.

9. Debido al incremento y a la continua aparición de nuevos virus, son eliminados automáticamente los mensajes con anexos susceptibles de ejecución.

10. Se limitará el tamaño máximo de los ficheros adjuntos y se asignará a los usuarios un tamaño máximo de buzón, dentro de unos límites razonables.

Artículo 22. Acceso a Internet desde la RCGVA

1. Condiciones de acceso a Internet.

a) El acceso a internet se realizará únicamente a través de la salida a internet establecida por el órgano con competencias en materia de tecnologías de la información utilizando los medios tecnológicos que se dispongan a tal fin.

b) El acceso a internet por otros medios, está expresamente prohibido.

c) Los recursos de internet serán filtrados 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.

d) Los perfiles de acceso serán creados por el órgano con competencias en materia de tecnologías de la información.

2. Responsabilidad del usuario final

a) La utilización de internet debe limitarse a la obtención de información relacionada con el trabajo que se desempeña, debiendo por lo tanto evitarse toda utilización que no tenga una mínima relación con las funciones encomendadas al usuario, o que pudiera conducir a una mejora en la calidad del trabajo desarrollado.

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

c) No se permite la descarga desde internet de cualquier clase de programas, aplicaciones, documentos o archivos que no provengan de páginas oficiales relacionadas con el trabajo, todo ello con la finalidad de que la descarga no pueda poner en peligro los sistemas informáticos y la información que la Generalitat custodia.

DISPOSICIONES FINALES

Primera. Desarrollo

Se autoriza al centro superior o directivo con competencias en materia de tecnologías de la información a dictar las instrucciones y órdenes de servicio, así como a adoptar las medidas que considere oportunas para el desarrollo y aplicación de la presente orden.

Segunda. Entrada en vigor

La presente orden entrará en vigor el día siguiente al de su publicación en el *Diari Oficial de la Comunitat Valenciana*.

Valencia, 3 de diciembre de 2013

El conseller de Hacienda y Administración Pública,
JUAN CARLOS MORAGUES FERRER

ANNEX
Glossari de termes

AMENANÇA: esdeveniments que poden desencadenar un incident en l'organització produint danys materials o pèrdues immaterials en els seus actius.

CONTRASENYA O CLAU D'ACCÉS: informació secreta, en general composta per un grup de caràcters, utilitzada per a l'autenticació.

CÒPIA DE SEGURETAT O SUPORT: còpia de les dades originals que es realitza a fi de disposar d'un mitjà de recuperar-les en cas de pèrdua.

DISPOSITIUS MÒBILS: un dispositiu mòbil es pot definir com un equip de dimensions xicotetes, amb algunes capacitats de processament, amb connexió permanent o intermitent a una xarxa, amb memòria limitada, que ha sigut dissenyat específicament per a una funció, però que poden dur a terme altres funcions més generals.

ENCRIPCIÓ: transformació criptogràfica de dades per a produir un criptograma o text encriptat.

EQUIP PORTÀTIL: és aquell ordinador personal que és capaç de realitzar la major part de les tasques que realitzen els ordinadors de sobretaula, amb capacitat semblant, amb l'avantatge del seu pes i grandària reduïts, així com la seua mobilitat.

IDENTIFICACIÓ D'ACCÉS: procés que limita i controla l'accés als recursos d'un sistema d'informació.

INFORMACIÓ SENSIBLE: aquella, així definida pel seu propietari, que ha de ser especialment protegida perquè la seua revelació, alteració, pèrdua o destrucció pot produir danys importants a algú o a alguna cosa.

MAQUINARI: es refereix a totes les parts tangibles d'un sistema informàtic; els seus components són elèctrics, electrònics, electromecànics i mecànics.

ORDINADORS PERSONALS: són els equips informàtics bàsics dels llocs de treball, on estaran instal·lades les aplicacions necessàries per a l'exercici de les funcions i des dels quals accedirà l'usuari a la xarxa corporativa i als sistemes d'informació.

PERFIL D'ACCÉS: limitació de l'accés als recursos exclusivament a persones, entitats o processos amb la deguda autorització.

TELEFONIA FIXA: és aquella que fa referència a les línies i equips que s'encarreguen de la comunicació entre terminals telefònics no portables, i generalment enllaçats entre ells o amb la central per mitjà de conductors metàl·lics.

XARXA CORPORATIVA DE LA GENERALITAT VALENCIANA (XCGVA): és la infraestructura comuna per a la interconnexió de les seues de totes les conselleries i organismes, tant en l'àmbit dels servicis de dades com de veu, amb distribució geogràfica que comprén tota la Comunitat Valenciana.

XARXA INFORMÀTICA: sistema de comunicació que connecta ordinadors i altres equips informàtics entre si, amb la finalitat de compartir informació i recursos.

XARXA SENSE FIL: la connexió d'equips per mitjà d'ones electromagnètiques i sense necessitat d'una connexió física per mitjà de cables. Les xarxes més usuals solen ser WI-FI, Bluetooth o infrarojos.

ANEXO
Glosario de términos

AMENAZA: eventos que pueden desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos.

CONTRASEÑA O CLAVE DE ACCESO: información secreta, en general compuesta por un grupo de caracteres, utilizada para la autenticación.

COPIA DE SEGURIDAD O RESPALDO: es una copia de los datos originales que se realiza con el fin de disponer de un medio de recuperarlos en caso de su pérdida.

DISPOSITIVOS MÓVILES: un dispositivo móvil se puede definir como un equipo de un tamaño pequeño, con algunas capacidades de procesamiento, con conexión permanente o intermitente a una red, con memoria limitada, que ha sido diseñado específicamente para una función, pero que pueden llevar a cabo otras funciones más generales.

CIFRADO: transformación criptográfica de datos para producir un criptograma o texto cifrado.

EQUIPO PORTÁTIL: es aquel ordenador personal que es capaz de realizar la mayor parte de las tareas que realizan los ordenadores de sobremesa, con similar capacidad, con la ventaja de su peso y tamaño reducidos, así como su movilidad.

IDENTIFICACIÓN DE ACCESO: proceso que limita y controla el acceso a los recursos de un sistema de información.

INFORMACIÓN SENSIBLE: aquella, así definida por su propietario, que debe ser especialmente protegida, pues su revelación, alteración, pérdida o destrucción puede producir daños importantes a alguien o a algo.

HARDWARE: se refiere a todas las partes tangibles de un sistema informático; sus componentes son: eléctricos, electrónicos, electromecánicos y mecánicos.

ORDENADORES PERSONALES: son los equipos informáticos básicos de los puestos de trabajo, donde estarán instaladas las aplicaciones necesarias para el desempeño de las funciones y desde los que accederá el usuario a la red corporativa y a los sistemas de información.

PERFIL DE ACCESO: limitación del acceso a los recursos exclusivamente a personas, entidades o procesos con la debida autorización.

TELEFONÍA FIJA: es aquella que hace referencia a las líneas y equipos que se encargan de la comunicación entre terminales telefónicos no portables, y generalmente enlazados entre ellos o con la central por medio de conductores metálicos.

RED CORPORATIVA DE LA GENERALITAT VALENCIANA (RCGVA): es la infraestructura común para la interconexión de las sedes de todas las consellerías y organismos, tanto a nivel de los servicios de datos como de voz, con distribución geográfica que abarca toda la Comunitat Valenciana.

RED INFORMÀTICA: sistema de comunicación que conecta ordenadores y otros equipos informáticos entre sí, con la finalidad de compartir información y recursos.

RED INALÀMBRICA: la conexión de equipos por medio de ondas electromagnéticas y sin necesidad de una conexión física mediante cables. Las redes más usuales suelen ser WIFI, Bluetooth, o infrarrojos.