Conselleria d'Hisenda i Model Econòmic

RESOLUCIÓ de 28 de març de 2018, de la Direcció General de Tecnologies de la Informació i les Comunicacions, per la qual s'estableixen els criteris d'estandardització tecnològica i les polítiques d'ús correcte del lloc de treball normalitzat dels usuaris TIC a l'Administració de la Generalitat i dels seus organismes autònoms. [2018/3769]

El Reglament orgànic i funcional de la Conselleria d'Hisenda i Model Econòmic (Decret 176/2016, de 25 de novembre, del Consell) atribueix a la Direcció General de Tecnologies de la Informació i les Comunicacions, DGTIC d'ara endavant, les competències de modernització, seguretat informàtica, planificació, coordinació, autorització i control de les tecnologies de la informació, les telecomunicacions i comunicacions corporatives i la teleadministració de la Generalitat.

Com a conseqüència de les regulacions bàsiques estatals o dels desplegaments normatius propis hi ha polítiques per a la protecció de dades de caràcter personal, per a l'ús segur de mitjans tecnològics a l'Administració de la Generalitat, tot això dins de l'Esquema Nacional de Seguretat. Els estàndards dels arxius (documents, àudios, vídeos, etc.) s'han desenvolupat dins de l'Esquema Nacional d'Interoperabilitat. Finalment, hi ha també una línia d'ús preferent del programari lliure derivada del mandat d'una moció de les Corts en 2016 en aqueix sentit.

El control de totes aquestes polítiques sectorials de seguretat, interoperabilitat i promoció de programari lliure, així com de les seues regulacions específiques ha de materialitzar-se i confluir necessàriament en la normalització de l'ús dels mitjans tecnològics posats a disposició dels usuaris de les tecnologies de la informació i les comunicacions de la Generalitat i dels seus organismes autònoms, usuaris TIC, d'ara endavant. És responsabilitat d'aquesta Direcció General l'estandardització de mitjans tecnològics de treball, la seua homologació i la creació de documents i normes que els arrepleguen i divulguen i donar-los, a més, el caràcter de compliment obligatori.

Per això, és convenient i necessari arreplegar en una resolució específica del Lloc de Treball Normalitzat totes les tasques de control i seguiment dels equips i els productes programari que hi estan instal·lats, la responsabilitat dels usuaris i els avanços en l'establiment d'algunes línies bàsiques d'una política de bones pràctiques exigible als dits usuaris dels mitjans tecnològics d'ús corporatiu.

Atés que els elements materials o equips i els productes programari que hi estan instal·lats hauran d'evolucionar per a adaptar-se a noves necessitats, la resolució preveu els corresponents annexos tècnics publicats i actualitzats en el portal de la DGTIC www.dgtic.gva.es.

Per tot això, resolc:

Primer. Objecte i àmbit de la resolució

La present resolució té per objecte la definició del Lloc de Treball Normalitzat com la integració dels elements materials dels equips assignats a cada usuari, dels elements programari instal·lats que es mostren en l'escriptori corporatiu (eines, aplicacions, accessos a documentació, etc.), així com les polítiques que regeixen l'ús adequat, segur i correcte del lloc de treball informàtic per a les finalitats administratives i corporatives de la Generalitat.

També és objecte d'aquesta resolució la determinació dels dits elements integrants del Lloc de Treball Normalitzat i de les polítiques aplicables a un ús correcte d'aquest.

L'àmbit d'aplicació de la present norma és l'Administració de la Generalitat i els seus organismes autònoms. S'exclou la Conselleria de Sanitat Universal i Salut Pública, de conformitat amb el Decret 37/ 2017, de 10 de març, del Consell, per la qual s'aprova el seu reglament orgànic i funcional.

Segon. Elements que integren els equips del Lloc de Treball Normalitzat

El Lloc de Treball Normalitzat es crea per a satisfer les necessitats d'equips i serveis tecnològics que demanden les unitats administratives

Conselleria de Hacienda y Modelo Económico

RESOLUCIÓN de 28 de marzo de 2018, de la Dirección General de Tecnologías de la Información y las Comunicaciones, por la que se establecen los criterios de estandarización tecnológica y las políticas de uso correcto del puesto de trabajo normalizado de los usuarios TIC en la Administración de la Generalitat y de sus organismos autónomos. [2018/3769]

El Reglamento orgánico y funcional de la Conselleria de Hacienda y Modelo Económico (Decreto 176/2016, de 25 de noviembre, del Consell) atribuye a la Dirección General de Tecnologías de la Información y las Comunicaciones, DGTIC en lo sucesivo, las competencias de modernización, seguridad informática, planificación, coordinación, autorización y control de las tecnologías de la información, las telecomunicaciones y comunicaciones corporativas y la teleadministración de la Generalitat.

Como consecuencia de las regulaciones básicas estatales o de los desarrollos normativos propios, existen políticas para la protección de datos de carácter personal, para el uso seguro de medios tecnológicos en la Administración de la Generalitat, todo ello dentro del Esquema Nacional de Seguridad. Los estándares de los archivos (documentos, audios, vídeos, etc) se han desarrollado dentro del Esquema Nacional de Interoperabilidad. Por último, existe también una linea de uso preferente del *software* libre derivada del mandato de una moción de Les Corts en 2016 en ese sentido.

El control de todas estas políticas sectoriales de seguridad, interoperabilidad y promoción de *software* libre así como de sus regulaciones específicas debe materializarse y confluye necesariamente en la normalización del uso de las medios tecnológicos puestos a disposición de los usuarios de las tecnologías de la información y las comunicaciones de la Generalitat y de sus organismos autónomos, usuarios TIC en los sucesivo. Es responsabilidad de esta Dirección General la estandarización de medios tecnológicos de trabajo, su homologación y la creación de documentos y normas que los recojan y divulguen, dándoles además el carácter de obligado cumplimiento.

Por ello, parece conveniente y necesario recoger en una resolución específica del Puesto de Trabajo Normalizado todas las tareas de control y seguimiento de los equipos y los productos *software* instalados en ellos, la responsabilidad de los usuarios y los avances en el establecimiento de algunas lineas básicas de una política de buenas prácticas exigible a dichos usuarios de los medios tecnológicos de uso corporativo.

Dado que los elementos materiales o equipos y los productos *software* instalados en ellos habrán de evolucionar para adaptarse a nuevas necesidades, la resolución prevé los correspondientes anexos técnicos publicados y actualizados en el portal de la DGTIC www.dgtic.gva.es.

Por todo ello, resuelvo:

Primero. Objeto y ámbito de la resolución

La presente resolución tiene por objeto la definición del Puesto de Trabajo Normalizado como la integración de los elementos materiales de los equipos asignados a cada usuario, de los elementos *software* instalados que se muestran en el escritorio corporativo (herramientas, aplicaciones, accesos a documentación, etc.), así como las políticas que rigen el uso adecuado, seguro y correcto del puesto de trabajo informático para las finalidades administrativas y corporativas de la Generalitat.

También es objeto de esta resolución la determinación de dichos elementos integrantes del Puesto de Trabajo Normalizado y de las políticas aplicables a un uso correcto del mismo.

El ámbito de aplicación de la presente norma es la Administración de la Generalitat y sus organismos autónomos. Se excluye a la Conselleria de Sanidad Universal y Salud Pública, de conformidad con el Decreto 37/ 2017, de 10 de marzo, del Consell, por la que se aprueba su Reglamento orgánico y funcional.

Segundo. Elementos que integran los equipos del Puesto de Trabajo Normalizado

El Puesto de Trabajo Normalizado se crea para satisfacer las necesidades de equipos y servicios tecnológicos que demandan las unida-

per als seus usuaris TIC i la DGTIC l'instal·la com a lloc de treball informàtic format dels elements següents:

1. Una CPU.
2. Una pantalla de visualització.
3. Un teclat.
4. Un dispositiu senyalador: ratolí, ratolí de bola, tauleta tàctil, etc.
5. Un sistema operatiu.
6. Un paquet ofimàtic estàndard.
7. Unes aplicacions homologades i autoritzades per la DGTIC necessàries per al tractament de la informació sota la seua competència.
8. Uns serveis finalistes i l'accés a aquests necessaris per al tractament de la informació sota la seua competència, per al manteniment del propi Lloc de Treball Normalitzat i per a assegurar la seguretat d'aquest.

Els llocs de treball informàtics que poden operar com a Lloc de Treball Normalitzat són els següents:

1. L'ordinador de sobretaula en qualsevol dels formats homologats per la DGTIC.
2. L'ordinador portàtil o convertible en qualsevol dels formats homologats per la DGTIC.
3. La tauleta tàctil en qualsevol dels formats homologats per la DGTIC.
4. Altres llocs de treball informàtics que la DGTIC declare com a homologats per al seu ús com a Lloc de Treball Normalitzat.

Tercer. Elements programari instal·lats en el Lloc de Treball Normalitzat

El Lloc de Treball Normalitzat requereix una sèrie de productes programari per a la seua operativitat, tant programari bàsic, sistema operatiu i ferramentes complementàries, com altres components necessaris per a l'accés a la xarxa corporativa i per a la interacció amb els aplicatius dels sistemes d'informació de l'Administració de la Generalitat i dels seus organismes autònoms.

La DGTIC mantindrà en el seu portal www.dgtic.gva.es una llista actualitzada i datada d'elements programari estàndards per al Lloc de Treball Normalitzat que estarà subjecta a revisions periòdiques. S'hi adjunta la versió en data d'entrada en vigor d'aquesta resolució en l'annex I Elements programari estàndards per al Lloc de Treball Normalitzat.

Per a conéixer les versions de cada programari que formen part del Lloc de Treball Normalitzat es tindrà en compte el pla de versions o pla de lliurament en els portals web de cada producte i s'acceptarà en el Lloc de Treball Normalitzat la versió actual amb suport en cada moment, la versió futura per a proves i diagnòstics (només en Lloc de Treball Normalitzat de proves) i la versió anterior per a facilitar l'adaptació d'altres aplicacions més complexes a les versions actuals.

Excepcionalment, i amb l'autorització prèvia per part de la DGTIC, es permetrà l'existència d'un programari en versions no actualitzades, sempre que no afecte l'arquitectura del Lloc de Treball Normalitzat en la seua versió actual pel que fa a la interacció amb altres aplicacions o eines.

Quart. L'emmagatzematge dels documents de treball

Els usuaris TIC d'un Lloc de Treball Normalitzat han d'emmagatzemar tots els documents de treball en els recursos compartits destinats a aquest propòsit per la DGTIC i no tenen permés emmagatzemar-los en dispositius o suports aliens a la xarxa corporativa, així com extraure'n còpies en qualsevol suport. Els dits recursos tenen la finalitat de restringir l'accés als documents, preservar la confidencialitat, auditar els accessos i ajudar i promocionar el treball col·laboratiu. A més, aquests recursos són els únics a què es proporciona còpia de seguretat per la qual cosa, davant de qualsevol incidència que afecte un document de forma accidental, podrà recuperar-se de manera autònoma o podrà sol·licitar-se la seua recuperació.

Els noms dels documents i les carpetes han de ser explicatius del seu contingut però eficients en la seua extensió atés que la ruta completa de l'arxiu no pot superar els 256 caràcters.

No està permés emmagatzemar informació privada de cap classe en els recursos compartits, ni en les unitats de xarxa, ni en les unitats locals, ni en cap altre mitjà o suport de la Generalitat.

des administrativas para sus usuarios TIC y la DGTIC lo instala como puesto de trabajo informático compuesto de los siguientes elementos:

1. Una CPU.
2. Una pantalla de visualización.
3. Un teclado.
4. Un dispositivo señalador: ratón, *trackball*, tableta, etc.
5. Un sistema operativo.
6. Un paquete ofimático estándar.
7. Unas aplicaciones homologadas y autorizadas por la DGTIC necesarias para el tratamiento de la información bajo su competencia.
8. Unos servicios finalistas y el acceso a los mismos necesarios para el tratamiento de la información bajo su competencia, para el mantenimiento del propio Puesto de Trabajo Normalizado y para asegurar la seguridad del mismo.

Los puestos de trabajo informáticos que pueden operar como Puesto de Trabajo Normalizado son los siguientes:

1. El ordenador de sobremesa en cualquiera de los formatos homologados por la DGTIC.
2. El ordenador portátil o convertible en cualquiera de los formatos homologados por la DGTIC.
3. La tableta en cualquiera de los formatos homologados por la DGTIC.
4. Otros puestos de trabajo informáticos que la DGTIC declare como homologados para su uso como Puesto de Trabajo Normalizado.

Tercero. Elementos software instalados en el Puesto de Trabajo Normalizado

El Puesto de Trabajo Normalizado requiere de una serie de productos *software* para su operatividad, tanto *software* básico, sistema operativo y herramientas complementarias, como otros componentes necesarios para el acceso a la red corporativa y para la interacción con los aplicativos de los sistemas de información de la Administración de la Generalitat y de sus organismos autónomos.

La DGTIC mantendrá en su portal www.dgtic.gva.es una lista actualizada y fechada de elementos *software* estándares para el Puesto de Trabajo Normalizado que estará sujeta a revisiones periódicas. Se adjunta la versión a fecha de entrada en vigor de esta resolución en el anexo I, «Elementos *software* estándares para el Puesto de Trabajo Normalizado».

Para conocer las versiones de cada *software* que forman parte del Puesto de Trabajo Normalizado, se tendrá en cuenta el plan de versiones o «release plan» en los portales web de cada producto, aceptándose en el Puesto de Trabajo Normalizado la versión actual con soporte en cada momento, la versión futura para pruebas y diagnósticos (solo en Puesto de Trabajo Normalizado de pruebas) y la versión anterior para facilitar la adaptación de otras aplicaciones más complejas a las versiones actuales.

Excepcionalmente, y previa autorización por parte de la DGTIC, se permitirá la existencia de un *software* en versiones no actualizadas, siempre y cuando no afecte a la arquitectura del Puesto de Trabajo Normalizado en su versión actual en lo que se refiere a la interacción con otras aplicaciones o herramientas.

Cuarto. El almacenamiento de los documentos de trabajo

Los usuarios TIC de un Puesto de Trabajo Normalizado deben almacenar todos los documentos de trabajo en los recursos compartidos destinados a este propósito por la DGTIC y no tienen permitido almacenarlos en dispositivos o soportes ajenos a la red corporativa, así como extraer copias de los mismos en cualquier soporte. Dichos recursos tienen la finalidad de restringir el acceso a los documentos, preservar la confidencialidad, auditar los accesos y ayudar y promocionar el trabajo colaborativo. Además, estos recursos son los únicos a los que se les proporciona copia de respaldo por lo que, ante cualquier incidencia que afecte a un documento de forma accidental, podrá recuperarse de manera autónoma o podrá solicitarse su recuperación.

Los nombres de los documentos y las carpetas deben ser explicativos de su contenido pero eficientes en su extensión dado que la ruta completa del archivo no puede superar los 256 caracteres.

No está permitido almacenar información privada de ninguna clase en los recursos compartidos, ni en las unidades de red, ni en las unidades locales, ni en ningún otro medio o soporte de la Generalitat.

Quan s'editen documents es recomana guardar canvis cada cert temps per a evitar la pèrdua d'aquesta informació en cas que sorgisca qualsevol problema tècnic.

L'estructura de recursos compartits està clarament definida en el domini GENERALITAT. En aquest es disposa de zones en què el propietari dels recursos pot establir l'estructura de directoris i a qui dóna permís per a accedir als seus recursos.

Cinqué. L'escriptori corporatiu del Lloc de Treball Normalitzat

Es defineix l'escriptori corporatiu com aquell en què es mostren als usuaris les eines i els accessos necessaris per al desenvolupament del seu treball i està format per una imatge de fons que segueix les normes d'identitat corporativa, una barra de tasques o accions, una sèrie d'icones, una tipografia, una resolució de pantalla predeterminada, un esquema de colors, un disseny de menú d'inici i un quadre d'informació del Lloc de Treball Normalitzat i de l'usuari.

L'escriptori corporatiu és d'obligada implantació en tots els Llocs de Treball Normalitzats i respon a criteris d'ergonomia comuna i d'imatge corporativa, com la interfície necessària entre l'usuari de les TIC i els sistemes d'informació de l'Administració de la Generalitat.

El fons corporatiu té la finalitat de mantindre la identitat corporativa de manera homogènia i coherent entre tot l'equipament propietat de l'Administració de la Generalitat. A més, el dit fons és el definit per al Lloc de Treball Normalitzat per la DGTIC en col·laboració amb la Direcció General de Relacions Informatives i Promoció Institucional, sota els estàndards d'identitat corporativa.

La resolució de pantalla estarà predeterminada, excepte en els casos en què la DGTIC autoritze alternatives per al millor ús d'alguna aplicació preexistent, a través del procediment que s'establisca des de la DGTIC. Per a aplicacions de desenvolupament posterior a aquesta resolució sobre el Lloc de Treball Normalitzat, aquestes hauran de preveure aquests estàndards.

En el fons de l'escriptori corporatiu i en la part inferior dreta, apareixerà sempre la informació relativa al Lloc de Treball Normalitzat, aquesta informació podrà ser sol·licitada pels tècnics de la DGTIC en cas d'incidència, motiu pel qual no es pot modificar ni eliminar.

S'exceptua el cas d'informe del Servei de Prevenció de Riscos Laborables en la línia de modificació de l'escriptori per motius de salut o ergonomia personalitzada i en aquest cas s'activarà el procediment per a la modificació d'aquest per a la persona o les persones afectades.

Sisé. Polítiques d'ús exigibles als usuaris del Lloc de Treball Normalitzat

1. Polítiques d'ús segur del Lloc de Treball Normalitzat

1.1. Amb caràcter general, la DGTIC proporcionarà als usuaris TIC de la Generalitat un compte personal i una contrasenya, o qualsevol altre procediment d'accés per característiques biomètriques, perquè el validen en el Lloc de Treball Normalitzat assignat. El dit compte serà personal i intransferible. L'usuari haurà de custodiar convenientment la seua identificació d'accés i serà responsable de qualsevol activitat relacionada amb l'ús del seu accés personal autoritzat, i en cap cas se subministrarà a terceres persones. L'incompliment del deure de custòdia del compte suposa una vulneració greu en la seguretat dels recursos TIC i per això es podria incórrer en responsabilitat.

La DGTIC mantindrà actualitzada la documentació que reflecteix la política de contrasenyes dels comptes d'usuari que ha de regir l'accés al Lloc de Treball Normalitzat dels usuaris TIC i la publicarà en el portal www.dgtic.gva.es amb detall de la seua data d'aprovació. S'adjunta en l'annex II la documentació respecte d'això que regeix en l'actualitat.

Quant al Lloc de Treball Normalitzat i amb caràcter general se seguiran les indicacions següents:

a) No es permet alterar la configuració del programari ni del sistema operatiu dels Llocs de Treball Normalitzats, ni desinstal·lar o instal·lar aplicacions, encara que siguen de programari lliure o gratuït, excepte als tècnics autoritzats per a això per la DGTIC.

b) Qualsevol programari privatiu ha de tindre la seua llicència legal associada, al corrent de pagament i custodiada per la DGTIC.

Cuando se editan documentos se recomienda guardar cambios cada cierto tiempo para evitar la pérdida de esta información en caso de surgir cualquier problema técnico.

La estructura de recursos compartidos esta claramente definida en el dominio GENERALITAT. En este, se dispone de zonas en las que el propietario de los recursos puede establecer la estructura de directorios y a quien le da permisos para acceder a sus recursos.

Quinto. El escritorio corporativo del Puesto de Trabajo Normalizado

Se define el escritorio corporativo como aquel en el que se muestran a los usuarios las herramientas y los accesos necesarios para el desarrollo de su trabajo y está formado por una imagen de fondo que sigue las normas de identidad corporativa, una barra de tareas o acciones, una serie de iconos, una tipografía, una resolución de pantalla predeterminada, un esquema de colores, un diseño de menú de inicio y un cuadro de información del Puesto de Trabajo Normalizado y del usuario.

El escritorio corporativo es de obligada implantación en todos los Puestos de Trabajo Normalizados y responde a criterios de ergonomía común y de imagen corporativa, como la interfaz necesaria entre el usuario de las TIC y los sistemas de información de la Administración de la Generalitat.

El fondo corporativo tiene la finalidad de mantener la identidad corporativa de manera homogénea y coherente entre todo el equipamiento propiedad de la Administración de la Generalitat. Además, dicho fondo es el definido para el Puesto de Trabajo Normalizado por la DGTIC en colaboración con la Dirección General de Relaciones Informativas y Promoción Institucional, bajo los estándares de identidad corporativa.

La resolución de pantalla vendrá predeterminada, salvo en los casos en que la DGTIC autorice alternativas para el mejor uso de alguna aplicación preexistente, a través del procedimiento que se establezca desde la DGTIC. Para aplicaciones de desarrollo posterior a esta Resolución sobre el Puesto de Trabajo Normalizado, estas deberán contemplar estos estándares.

En el fondo del escritorio corporativo y en su parte inferior derecha, aparecerá siempre la información relativa al Puesto de Trabajo Normalizado, esta información podrá ser solicitada por los técnicos de la DGTIC en caso de incidencia, motivo por el cual no se puede modificar ni eliminar.

Se excepciona el caso de informe del Servicio de Prevención de Riesgos Laborables en la línea de modificación del escritorio por motivos de salud o ergonomía personalizada, en cuyo caso se activará el procedimiento para la modificación del mismo para la o las personas afectadas.

Sexto. Políticas de uso exigibles a los usuarios del Puesto de Trabajo Normalizado

1. Políticas de uso seguro del Puesto de Trabajo Normalizado

1.1. Con carácter general, la DGTIC proporcionará a los usuarios TIC de la Generalitat una cuenta personal y una contraseña, o cualquier otro procedimiento de acceso por características biométricas, para validarse en el Puesto de Trabajo Normalizado asignado. Dicha cuenta será personal e intransferible, debiendo el usuario custodiar convenientemente su identificación de acceso, siendo responsable de toda la actividad relacionada con el uso de su acceso personal autorizado, y en ningún caso se suministrará a terceras personas. El incumplimiento del deber de custodia de la cuenta supone una vulneración grave en la seguridad de los recursos TIC y por ello se podría incurrir en responsabilidad.

La DGTIC mantendrá actualizada la documentación que refleja la política de contraseñas de las cuentas de usuario que debe regir el acceso al Puesto de Trabajo Normalizado de los usuarios TIC y la publicará en su portal www.dgtic.gva.es con detalle de su fecha de aprobación. Se adjunta en el Anexo II la documentación al respecto que rige en la actualidad.

En relación con el Puesto de Trabajo Normalizado y con carácter general se seguirán las siguientes indicaciones:

a) No se permite alterar la configuración del *software* ni del sistema operativo de los Puestos de Trabajo Normalizados, ni desinstalar o instalar aplicaciones, aunque sean de *software* libre o gratuito, salvo a los técnicos autorizados para ello por la DGTIC.

b) Todo *software* privativo debe tener su licencia legal asociada, al corriente de pago y custodiada por la DGTIC.

c) No es permet l'alteració de la configuració física dels Llocs de Treball Normalitzats, ni del seu microprogramari, ni connectar cap dispositiu a iniciativa de l'usuari, com tampoc variar-ne la ubicació, excepte als tècnics autoritzats per a això per la DGTIC. L'equipament informàtic no és propietat de l'usuari, és un element de la plaça laboral que ocupa i pertany a l'Administració de la Generalitat.

d) No es permet emmagatzemar informació el tractament del qual siga responsabilitat de l'Administració de la Generalitat en mode local o dispositius externs connectats als Llocs de Treball Normalitzats, han d'utilitzar-se els recursos descrits en el primer paràgraf del punt quart d'aquesta resolució o les aplicacions dissenyades per a això per la Generalitat.

e) Els equips informàtics no estan destinats a l'ús personal de l'usuari.

f) Al connectar-se un dispositiu d'emmagatzematge extern prèviament autoritzat per la DGTIC, es tindrà la precaució de realitzar un escaneig amb l'antivirus sobre la dita unitat per a previndre una possible infecció dels sistemes informàtics.

g) És obligatori bloquejar la sessió de l'usuari en el supòsit d'absentar-se temporalment del lloc de treball, a fi d'evitar accessos d'altres persones a l'equip informàtic.

h) En acabar la jornada laboral l'usuari TIC haurà d'apagar completament el Lloc de Treball Normalitzat i tots els seus perifèrics connectats o relacionats amb aquest.

En qualsevol cas i en la mesura que siga possible la DGTIC s'assegurarà del compliment d'aquestes mesures amb els mitjans tecnològics al seu abast.

1.2. A més de les normes d'ús del punt anterior amb caràcter general, en l'ús dels dispositius portables s'està sotmés a les obligacions següents:

a) No s'emmagatzemarà informació sensible o confidencial en aquest tipus de dispositius, i en cas que siga absolutament necessari, haurà de ser protegida per mitjà d'eines de xifrat amb la sol·licitud prèvia a la DGTIC. No obstant això, aquells dispositius que ho permeten i seguint el que disposa l'Ordre 19/2013, de 3 de desembre, de la Conselleria d'Hisenda i Administració Pública, per la qual s'estableixen les normes sobre l'ús segur de mitjans tecnològics en l'Administració de la Generalitat, tindran tots els seus elements d'emmagatzematge xifrats.

b) Aquest tipus de dispositius estarà sota la custòdia de l'usuari TIC que els utilitze. No es deixarà el Lloc de Treball Normalitzat desatés o abandonat en llocs on puga ser sostret.

c) La pèrdua o robatori de qualsevol dispositiu d'aquest tipus s'haurà de notificar immediatament al responsable corresponent i aquest a la DGTIC.

d) Els usuaris TIC d'aquests equips es responsabilitzaran que no seran usats per terceres persones alienes a la Generalitat o no autoritzades per a això.

e) Es proporcionarà accés remot a recursos interns de la Generalitat només en els casos que estiga degudament justificat i, a més, se seguisca el procediment aprovat a aquest efecte per la DGTIC.

1.3. A més del que preveu l'apartat 1, amb caràcter general, els dispositius d'emmagatzematge extern proporcionats per la Generalitat seran els únics autoritzats, seran conformes a les normes de seguretat d'aquesta i seran destinats a un ús exclusivament professional, com a eina de transport de fitxers i mai com a eina d'emmagatzematge.

a) No està permés l'emmagatzematge d'informació sensible o confidencial en aquest tipus de suport. En cas que siga estrictament necessari emmagatzemar aquest tipus d'informació classificada, haurà de tindre l'autorització del responsable del fitxer en el cas de dades personals i haurà de ser protegida per mitjà d'eines de xifrat amb la sol·licitud prèvia a la DGTIC.

b) Aquest tipus de dispositius estarà sota la custòdia de l'usuari TIC que els utilitze. No es deixarà el dispositiu d'emmagatzematge extern desatés o abandonat en llocs on puga ser sostret.

c) La pèrdua o robatori del dispositiu d'emmagatzematge extern haurà de notificar-se immediatament al responsable corresponent i aquest a la DGTIC.

2. Polítiques de tractament de la informació

De conformitat amb la legislació vigent, no està permés el tractament de dades de caràcter personal sense que prèviament haja sigut

c) No se permite la alteración de la configuración física de los Puestos de Trabajo Normalizados, ni de su «*firmware*», ni conectar ningún dispositivo a iniciativa del usuario, así como variar la ubicación del mismo, salvo a los técnicos autorizados para ello por la DGTIC. El equipamiento informático no es propiedad del usuario, es un elemento de la plaza laboral que ocupa y pertenece a la Administración de la Generalitat.

d) No se permite almacenar información cuyo tratamiento sea responsabilidad de la Administración de la Generalitat en modo local o dispositivos externos conectados a los Puestos de Trabajo Normalizados, deben emplearse los recursos descritos en primer párrafo del punto Cuarto de esta Resolución o las aplicaciones diseñadas para ello por la Generalitat.

e) Los equipos informáticos no están destinados al uso personal del usuario.

f) Al conectarse un dispositivo de almacenamiento externo previamente autorizado por la DGTIC, se tendrá la precaución de realizar un escaneo con el antivirus sobre dicha unidad para prevenir una posible infección de los sistemas informáticos.

g) Es obligatorio bloquear la sesión del usuario en el supuesto de ausentarse temporalmente del lugar de trabajo, a fin de evitar accesos de otras personas al equipo informático.

h) Al terminar la jornada laboral el usuario TIC deberá apagar completamente el Puesto de Trabajo Normalizado y todos sus periféricos conectados o relacionados con él.

En cualquier caso y en la medida de lo posible la DGTIC se asegurará del cumplimiento de estas medidas con los medios tecnológicos a su alcance.

1.2. Además de las normas de uso del punto anterior con carácter general, en el uso de los dispositivos portables se está sometido las obligaciones siguientes:

a) No se almacenará información sensible o confidencial en este tipo de dispositivos, y en caso de ser absolutamente necesario, deberá ser protegida mediante herramientas de cifrado previa solicitud a la DGTIC. No obstante, aquellos dispositivos que lo permitan y siguiendo lo dispuesto por la Orden 19/2013, de 3 de diciembre, de la Conselleria 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, tendrán todos sus elementos de almacenamiento cifrados.

b) Este tipo de dispositivos estará bajo la custodia del usuario TIC que los utilice. No se dejará el Puesto de Trabajo Normalizado desatendido o abandonado en lugares donde pueda ser sustraído.

c) La pérdida o robo de cualquier dispositivo de este tipo deberá notificarse de inmediato al responsable correspondiente y este a la DGTIC.

d) Los usuarios TIC de estos equipos se responsabilizarán de que no serán usados por terceras personas ajenas a la Generalitat o no autorizadas para ello.

e) Se proporcionará acceso remoto a recursos internos de la Generalitat solo en los casos que esté debidamente justificado y además se siga el procedimiento aprobado a tal efecto por la DGTIC.

1.3. Además de lo previsto en el apartado 1. con carácter general, los dispositivos de almacenamiento externo proporcionados por la Generalitat serán los únicos autorizados, serán conformes a las normas de seguridad de esta, y serán destinados a un uso exclusivamente profesional, como herramienta de transporte de ficheros y nunca como herramienta de almacenamiento.

a) No está permitido el almacenamiento de información sensible o confidencial en este tipo de soporte. En caso de ser estrictamente necesario almacenar este tipo de información clasificada, deberá tener la autorización del responsable del fichero en el caso de datos personales, y debe ser protegida mediante herramientas de cifrado previa solicitud a la DGTIC.

b) Este tipo de dispositivos estará bajo la custodia del usuario TIC que los utilice. No se dejará el dispositivo de almacenamiento externo desatendido o abandonado en lugares donde pueda ser sustraído.

c) La pérdida o robo del dispositivo de almacenamiento externo deberá notificarse de inmediato al responsable correspondiente y este a la DGTIC.

2. Políticas de tratamiento de la Información

De conformidad con la legislación vigente, no está permitido el tratamiento de datos de carácter personal sin que previamente haya sido

autoritzat per l'òrgan responsable del fitxer en la forma reglamentàriament prevista ni podran usar-se per a finalitats diferents d'aquelles per a les quals les dades hagueren sigut obtingudes.

Està prohibit utilitzar, 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.

3. Polítiques de bones pràctiques de l'usuari TIC

3.1. En l'ús del Lloc de Treball Normalitzat els usuaris TIC han de respectar l'ordenament jurídic aplicable i els drets reconeguts en la Constitució Espanyola. Per això, no és correcta, i pot derivar en responsabilitat de l'usuari del Lloc de Treball Normalitzat, la utilització del Lloc de Treball Normalitzat per a una, alguna o totes les finalitats següents:

a) Incórrer en activitats il·lícites o il·legals de qualsevol tipus i, particularment, difondre continguts de caràcter racista, xenòfob, pornogràfic, sexista, d'apologia del terrorisme, que atempten contra els drets humans o que actuen en perjuí dels drets a la intimitat, a l'honor, a la pròpia imatge o contra la dignitat de les persones.

b) Difondre continguts contraris als principis enunciats en l'ordenament jurídic.

c) Difondre afirmacions o referències falses, incorrectes o inexactes sobre l'Administració de la Generalitat, els seus centres, departaments i serveis, així com les activitats que desenvolupa.

d) Congestionar intencionadament la xarxa corporativa de la Generalitat o interferir en el seu funcionament.

e) Establir mecanismes o sistemes que permeten aprofitaments indeguts dels recursos de xarxa proporcionats per la Generalitat per tercers, com revendre'ls o reutilitzar-los per a finalitats privades, lucratives o delictives, entre altres.

f) Danyar els sistemes físics i lògics de l'Administració de la Generalitat, introduir o difondre en la xarxa virus informàtics i realitzar qualsevol altre tipus d'activitat que siga susceptible de provocar danys en l'Administració de la Generalitat, als seus membres, proveïdors o terceres persones.

g) Tractar dades personals contingudes en fitxers que no siguen responsabilitat de l'Administració de la Generalitat.

h) Arreplegar dades personals, tant de manera directa com mitjançant tractaments invisibles, excepte aquelles que estiguen directament relacionades amb les funcions pròpies de l'Administració de la Generalitat, o realitzar qualsevol tractament de dades personals que no siguen titularitat de l'Administració de la Generalitat i per al qual no haja sigut prèviament autoritzat.

i) Publicar o difondre dades, documents o arxius que afecten terceres persones o que estiguen subjectes en drets de privacitat o propietat intel·lectual o qualsevol altres drets o interessos legítims, sense el consentiment exprés de les persones afectades o del titular dels drets.

j) Fer ús dels recursos TIC amb fins comercials.

k) Enviar comunicacions amb finalitats comercials o correu massiu no sol·licitat amb finalitats publicitàries (correu brossa) des dels comptes de correu electrònic de la Generalitat.

l) Vulnerar els drets de propietat intel·lectual o industrial de tercers.

3.2. En relació amb la responsabilitat de l'usuari TIC en l'accés a internet:

L'usuari TIC s'atindrà a les normes d'ús següents:

a) La utilització d'internet s'ha de limitar a l'obtenció d'informació relacionada amb el treball que es realitza com a empleat o empleada pública al servei de l'Administració de la Generalitat i els seus organismes autònoms o a l'execució d'aplicacions corporatives desenvolupades o habilitades per a aquesta finalitat.

b) En particular, no està permés l'accés a pàgines web de contingut ofensiu, inapropiat, pornogràfic o discriminatori per raons de gènere, ètnia, opció sexual, discapacitat o qualsevol altra circumstància personal o social, excepte per a funcions de detecció i persecució del delicte, que requerirà d'autorització expressa per part de la DGTIC.

c) No es permet la descàrrega des d'internet de qualsevol classe de programes, aplicacions, documents o arxius.

4. Polítiques d'ús dels certificats digitals en el Lloc de Treball Normalitzat

autorizado por el órgano responsable del fichero en la forma reglamentariamente prevista ni podrán usarse para finalidades distintas de aquellas para las que los datos hubieran sido obtenidos.

Está prohibido utilizar, copiar, extraer o trasmitir información contenida en el sistema informático, para uso privado o para cualquier otro distinto del servicio público al que está destinada.

3. Políticas de buenas prácticas del usuario TIC

3.1. En el uso del Puesto de Trabajo Normalizado los usuarios TIC han de respetar el ordenamiento jurídico aplicable y los derechos reconocidos en la Constitución española. Por ello, no es correcta, y puede derivar en responsabilidad del usuario del Puesto de Trabajo Normalizado, la utilización del Puesto de Trabajo Normalizado para una, alguna o todas las finalidades siguientes:

a) Incurrir en actividades ilícitas o ilegales de cualquier tipo y, particularmente, difundir contenidos de carácter racista, xenófobo, pornográfico, sexista, de apología del terrorismo, que atentan contra los derechos humanos o que actúan en perjuicio de los derechos a la intimidad, al honor, a la propia imagen o contra la dignidad de las personas.

b) Difundir contenidos contrarios a los principios enunciados en el ordenamiento jurídico.

c) Difundir afirmaciones o referencias falsas, incorrectas o inexactas sobre la Administración de la Generalitat, sus centros, departamentos y servicios, así como las actividades que desarrolla.

d) Congestionar intencionadamente la red corporativa de la Generalitat o interferir en su funcionamiento.

e) Establecer mecanismos o sistemas que permiten aprovechamientos indebidos de los recursos de red proporcionados por la Generalitat por terceros, como revenderlos o reutilizarlos para finalidades privadas, lucrativas o delictivas, entre otras.

f) Dañar los sistemas físicos y lógicos de la Administración de la Generalitat, introducir o difundir en la red virus informáticos y realizar cualquiera otro tipo de actividad que sea susceptible de provocar daños en la Administración de la Generalitat, a sus miembros, proveedores o terceras personas.

g) Tratar datos personales contenidos en ficheros que no sean responsabilidad de la Administración de la Generalitat.

h) Recoger datos personales, tanto de manera directa cómo intermediando tratamientos invisibles, excepto aquellas que estén directamente relacionadas con las funciones propias de la Administración de la Generalitat, o realizar cualquier tratamiento de datos personales que no sean titularidad de la Administración de la Generalitat y para el que no haya sido previamente autorizado.

i) Publicar o difundir datos, documentos o archivos que afectan a terceras personas o que estén sujetas en derechos de privacidad o propiedad intelectual o cualesquier otros derechos o intereses legítimos, sin el consentimiento expreso de las personas afectadas o del titular de los derechos.

j) Hacer uso de los recursos TIC con fines comerciales.

k) Enviar comunicaciones con finalidades comerciales o correo masivo no solicitado con finalidades publicitarias (SPAM) desde las cuentas de correo electrónico de la Generalitat.

l) Vulnerar los derechos de propiedad intelectual o industrial de terceros.

3.2. En relación con la responsabilidad del usuario TIC en el acceso a internet:

El usuario TIC se atendrá a la siguientes normas de uso:

a) La utilización de internet debe limitarse a la obtención de información relacionada con el trabajo que se desempeña como empleado o empleada pública al servicio de la Administración de la Generalitat y sus organismos autónomos o a la ejecución de aplicaciones corporativas desarrolladas o habilitadas para tal fin.

b) En particular, no está permitido el acceso a páginas web de contenido ofensivo, inapropiado, pornográfico o discriminatorio por razones de género, etnia, opción sexual, discapacidad o cualquier otra circunstancia personal o social, excepto para funciones de detección y persecución del delito, que requerirá de autorización expresa por parte de la DGTIC.

c) No se permite la descarga desde internet de cualquier clase de programas, aplicaciones, documentos o archivos.

4. Políticas de uso de los certificados digitales en el Puesto de Trabajo Normalizado

Els certificats digitals són sempre personals i és responsabilitat de l'usuari la sol·licitud, instal·lació, custòdia i revocació d'aquests.

Es tindrà present en totes les actuacions que els certificats digitals s'hauran d'instal·lar sempre amb un nivell alt de seguretat, perquè se sol·licite la contrasenya d'ús cada vegada que siga necessari utilitzar-lo. Si el certificat digital va amb targeta de firma electrònica, aquesta no s'ha de deixar oblidada en els lectors de targeta, ja siga en el teclat o independents, i haurà de romandre sempre sota la custòdia del titular del certificat digital.

No s'ha de facilitar, en cap concepte, el codi d'accés del certificat digital.

En previsió que puga donar-se un esborrament de dades en el Lloc de Treball Normalitzat o una avaria que suposara la pèrdua del certificat, es recomana realitzar-ne una còpia de seguretat per a evitar sol·licitar novament el certificat digital.

En el cas que un servei, una aplicació o un tercer, sol·licite l'arxiu del certificat en format «.pfx», no ha de ser facilitat en cap concepte, atés que aquest format conté la clau privada del certificat i pot permetre la suplantació.

5. Polítiques d'actualització contínua del Lloc de Treball Normalitzat

Els departaments de personal de l'Administració de la Generalitat i dels seus organismes autònoms i les unitats administratives, quan es tracta de persones que desenvolupen tasques contractades, estan obligats a comunicar les variacions d'estat quan un Lloc de Treball Normalitzat deixe d'estar assignat a un usuari TIC per canvi d'adscripció o finalització de tasques.

A partir de la dita comunicació, la DGTIC procedirà a l'anul·lació del Lloc de Treball Normalitzat creat per a l'usuari cessant, la qual cosa inclou els mitjans i les instal·lacions tecnològics que se li hagueren assignat, per a deixar lliures els equips per a nou ús. També s'inclouen les claus, certificats instal·lats i els comptes de correu corporatius.

Els canvis simples d'ubicació en departaments o edificis també han de ser comunicats pels departaments de personal o per les unitats administratives que els autoritzen amb la mateixa finalitat de control i actualització permanent dels recursos TIC disposats per part de la DGTIC.

Seté. Obligat compliment i responsabilitat de l'usuari del Lloc de Treball Normalitzat

Tot el que es preveu en aquesta resolució quant al Lloc de Treball Normalitzat és de compliment obligatori per als usuaris TIC de la Generalitat i els seus organismes autònoms en l'àmbit de competències d'aquesta Direcció General.

Per això, en accedir a l'equip per a l'inici d'una sessió en un Lloc de Treball Normalitzat, i com a primera imatge emergent, es mostrarà un resum del que estableix aquesta resolució per a la seua lectura i acceptació per l'usuari. L'acceptació tàcita i, per tant, la responsabilitat de l'usuari es considera implícita en iniciar el seu treball en la sessió.

En aquells enunciats d'aquesta resolució que incideixen en aspectes de prohibicions o limitacions en l'ús del Lloc de Treball Normalitzat és d'aplicació el règim sancionador general per al personal propi. Quant a incidències dels usuaris TIC en els processos de desenvolupaments contractats amb empreses adjudicatàries, caldrà ajustar-se al que prevegen quant a responsabilitat d'aquests en el corresponent plec de contractació.

En els supòsits d'incidents referits a les dades personals, la propietat intel·lectual, la seguretat informàtica i altres aspectes regulats per altres disposicions legals diferents de la present resolució, el règim sancionador serà el corresponent a aqueixes disposicions normatives.

Huité. Publicació i efectivitat de la resolució

La present resolució entrarà en vigor l'endemà de la seua publicació en el *Diari Oficial de la Generalitat Valenciana.*

València, 28 de març de 2018.– El director general de Tecnologies de la Informació i les Comunicacions: Pedro Agustín Pernias Peco.

Los certificados digitales son siempre personales y es responsabilidad del usuario la solicitud, instalación, custodia y revocación de los mismos.

Se tendrá presente en todas las actuaciones que los certificados digitales se deberán instalar siempre con nivel alto de seguridad, para que se solicite la contraseña de uso cada vez que sea necesario utilizarlo. Si el certificado digital viene en tarjeta de firma electrónica, esta no se debe dejar olvidada en los lectores de tarjeta, ya sea en teclado o independientes, y deberá permanecer siempre bajo custodia del titular del certificado digital.

No se debe facilitar, bajo ningún concepto, el código de acceso del certificado digital.

En prevención de que pueda darse un borrado de datos en el Puesto de Trabajo Normalizado o una avería que supusiese la pérdida del certificado, se recomienda realizar una copia de seguridad para evitar solicitar de nuevo su certificado digital.

En caso de que un servicio, una aplicación o un tercero, solicite el archivo del certificado en formato «.pfx», no debe ser facilitado bajo ningún concepto, dado que este formato contiene la clave privada del certificado y puede permitir la suplantación.

5. Políticas de actualización continua del Puesto de Trabajo Normalizado

Los departamentos de personal de la Administración de la Generalitat y de sus organismos autónomos y las unidades administrativas, cuando se trata de personas que desarrollan tareas contratadas, están obligados a comunicar las variaciones de estado cuando un Puesto de Trabajo Normalizado deje de estar asignado a un usuario TIC por cambio de adscripción o terminación de tareas.

A partir de dicha comunicación, la DGTIC procederá a la anulación del Puesto de Trabajo Normalizado creado para el usuario cesante, lo cual incluye los medios e instalaciones tecnológicos que se le hubieran asignado, para dejar libres los equipos para nuevo uso. También se incluyen las claves, certificados instalados y las cuentas de correo corporativas.

Los cambios simples de ubicación en departamentos o edificios también deben ser comunicados por los departamentos de personal o por las unidades administrativas que los autoricen con la misma finalidad de control y actualización permanente de los recursos TIC dispuestos por parte de la DGTIC.

Séptimo. Obligado cumplimiento y responsabilidad del usuario del Puesto de Trabajo Normalizado

Todo lo que se prevé en esta Resolución en cuanto al Puesto de Trabajo Normalizado es de obligado cumplimiento para los usuarios TIC de la Generalitat y sus organismos autónomos en el ámbito de competencias de esta Dirección General.

Por ello, al acceder al equipo para el inicio de una sesión en un Puesto de Trabajo Normalizado, y como primera imagen emergente, se mostrará un resumen de lo previsto en esta Resolución para su lectura y aceptación por el usuario. La aceptación tácita y, por tanto, la responsabilidad del usuario se considera implícita al iniciar su trabajo en la sesión.

En aquellos enunciados de esta resolución que inciden en aspectos de prohibiciones o limitaciones en el uso del Puesto de Trabajo Normalizado, es de aplicación el Régimen Sancionador General para el personal propio. En cuanto a incidencias de los usuarios TIC en los procesos de desarrollos contratados con empresas adjudicatarias, se estará a lo que prevean en cuanto a responsabilidad de estas en el correspondiente pliego de contratación.

En los supuestos de incidentes referidos a los datos personales, la propiedad intelectual, la seguridad informática y otros aspectos regulados por otras disposiciones legales distintas a la presente resolución, el régimen sancionador será el correspondiente a esas disposiciones normativas.

Octavo. Publicación y efectividad de la resolución

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

València, 28 de marzo de 2018.– El director general de Tecnologías de la Información y las Comunicaciones: Pedro Agustín Pernias Peco.

ANNEX I

Elements programari estàndards per al Lloc de Treball Normalitzat

Versió data 5 de març de 2018

El present annex es distribueix en 3 taules que representen els tres components bàsics del Lloc de Treball Normalitzat quant a programari: sistemes operatius, programari bàsic i remediacions.

ANEXO I

Elementos software *estándares para el Puesto de Trabajo Normalizado*

Versión de fecha 5 de marzo de 2018

El presente anexo se distribuye en 3 tablas que representan los tres componentes básicos del Puesto de Trabajo Normalizado en cuanto a *software*: sistemas operativos, software básico y remediaciones.

Sistemes operatius

Nom del programari	*Codi: Lloc de treball Normalitzat (PTN)*	*Versió*	*Fi de vida*
Lliurex Administració	PTN ELC	15.05, 64 bits	2018
Microsoft Windows[1]	PTN EPC	7 Pro SP1, 64 bits	2019
Microsoft Windows	PTN EPC	10 E3/Pro, 64 bits	2030

Programari bàsic

Nom software	*Versió en PTN SOP Windows*	*Versió en PTN SOP LliureX*	*Tipus*	*Fi de vida*
Libre Office	Última estable[2]		Ofimàtica	2018
Mozilla Firefox	Última estable ESR[3]		Internet	2018
Mozilla Thunderbird	Última estable[4]		Missatgeria	2018
Lightning Thunderbird	Integrat amb Thunderbird		Ofimàtica	2018
Adobe Acrobat Reader	Última estable		Utilitat	2018
McAfee Antivirus	Última estable	No en requereix	Infraestructura	2019
Salt	Última estable		Utilitat	–
WinAudit	Última estable	No en requereix	Infraestructura	–
OCS Inventory	No requereix	Última estable	Infraestructura	–
Escriptori remot integrat	Última estable	No en requereix	Infraestructura	–
Escriptori remot Xrdp	No en requereix	Última estable	Infraestructura	–
VLC Player	Última estable		Multimèdia	2018
Java con Deployment Ruleset	Última estable[5]		Tecnologia	2018
Adobe Flash Player	Última estable[6]		Tecnologia	2018
7-zip	Última estable		Utilitat	–
Visor d' imatges (en el SO)	Integrat en el SO		Multimèdia	–
PDF Creator	Última estable	No en requereix	Utilitat	–
FreeOCR	Última estable	–	Utilitat	–
BGInfo	Última estable	–	Infraestructura	–
Lectors Targetes Cripto: Cherry	Última estable	No en requereix	Infraestructura	–
Lectors Targetes Cripto: Omnikey	Última estable	No en requereix	Infraestructura	–
Lectors Targetes Cripto: SCR3	Última estable	No en requereix	Infraestructura	–
Targetes Cripto: G&D	Última estable	–	Infraestructura	–
Targetes Cripto: DNIe	Última estable	–	Infraestructura	–
Targetes Cripto: FNMT	Última estable	–	Infraestructura	–

1 La versió *Microsoft Windows 7* desapareixerà com a estàndard el 14 de gener de 2020, data en què finalitza el suport estés. La DGTIC està planificant la migració a *Microsoft Windows 10* per a abans d'aqueixa data.

2 La versió de Libre*Office* estàndard és l'última publicada amb qualitat «*STILL*» per «*The Document Foudation*».

3 La versió de *Firefox* estàndard és l'última publicada amb qualitat «*ESR*» per «*The Mozilla Foundation*».

4 La versió de *Thunderbird* és l'última publicada amb qualitat estables pel projecte *Thunderbird*.

5 La versió de *Java* serà l'última estable i amb suport «d'Oracle *Corporation*».

6 La versió de *Adobe Flash* serà l'última estable i amb suport «d'Adobe *Systems Incorporated*».

Sistemas Operativos

Nombre del software	*Código: Puesto de trabajo Normalizado (PTN)*	*Versión*	*Fin de Vida*
Lliurex Administración	PTN ELC	15.05, 64bits	2018
Microsoft Windows[1]	PTN EPC	7 Pro SP1, 64bits	2019
Microsoft Windows	PTN EPC	10 E3/Pro, 64bits	2030

Software Básico

Nombre software	*Versión en PTN SOP Windows*	*Versión en PTN SOP LliureX*	*Tipo*	*Fin de Vida*
Libre Office	Última estable[2]		Ofimática	2018
Mozilla Firefox	Última estable ESR[3]		Internet	2018
Mozilla Thunderbird	Última estable[4]		Mensajería	2018
Lightning Thunderbird	Integrado con Thunderbird		Ofimática	2018
Adobe Acrobat Reader	Última estable		Utilidad	2018
McAfee Antivirus	Última estable	No requiere	Infraestructura	2019
Salt	Última estable		Utilidad	–
WinAudit	Última estable	No requiere	Infraestructura	–
OCS Inventory	No requiere	Última estable	Infraestructura	–
Escritorio remoto integrado	Última estable	No requiere	Infraestructura	–
Escritorio remoto Xrdp	No requiere	Última estable	Infraestructura	–
VLC Player	Última estable		Multimedia	2018
Java con Deployment Ruleset	Última estable[5]		Tecnología	2018
Adobe Flash Player	Última estable[6]		Tecnología	2018
7-zip	Última estable		Utilidad	–
Visor de imágenes (en el SO)	Integrado en el SO		Multimedia	–
PDF Creator	Última estable	No requiere	Utilidad	–
FreeOCR	Última estable	–	Utilidad	–
BGInfo	Última estable	–	Infraestructura	–
Lectores Tarjetas Cripto: Cherry	Última estable	No requiere	Infraestructura	–
Lectores Tarjetas Cripto: Omnikey	Última estable	No requiere	Infraestructura	–
Lectores Tarjetas Cripto: SCR3	Última estable	No requiere	Infraestructura	–
Tarjetas Cripto: G&D	Última estable	–	Infraestructura	–
Tarjetas Cripto: DNIe	Última estable	–	Infraestructura	–
Tarjetas Cripto: FNMT	Última estable	–	Infraestructura	–

1 La versión *Microsoft Windows 7* desaparecerá como estándar el 14 de enero de 2020, fecha en la que finaliza el soporte extendido. La DGTIC está planificando la migración a *Microsoft Windows 10* para antes de esa fecha.
2 La versión de Libre*Office* estándar es la última publicada con calidad «*STILL*» por *«The Document Foudation*».
3 La versión de *Firefox* estándar es la última publicada con calidad «*ESR*» por «*The Mozilla Foundation*».
4 La versión de *Thunderbird* es la última publicada con calidad estables por el proyecto *Thunderbird*.
5 La versión de *Java* será la última estable y con soporte de «*Oracle Corporation*».
6 La versión de *Adobe Flash* será la última estable y con soporte de «*Adobe Systems Incorporated*».

Remediacions

Quant a programari les remediacions es divideixen en dos categories principals: Sistema Operatiu i Tecnologia.

Sistemes Operatius

Nom del programari	*Codi PTN*	*Versió*	*Fi de vida*
Lliurex Administració	PTN ELC32	15.05, 32 bits	2018
Microsoft Windows	PTN EPC32	7 Pro SP1, 32 bits	2019
Microsoft Windows	PTN EPC32	10 E3/Pro, 32 bits	2030

Remediaciones

En cuanto a *software* las remediaciones se dividen en dos categorías principales: Sistema Operativo y Tecnología.

Sistemas Operativos

Nombre del software	Código PTN	Versión	Fin de vida
Lliurex Administración	PTN ELC32	15.05, 32bits	2018
Microsoft Windows	PTN EPC32	7 Pro SP1, 32bits	2019
Microsoft Windows	PTN EPC32	10 E3/Pro, 32bits	2030

Tecnologia

Nom del programari	*Versió en PTN EPC*	*Versió en PTN ELC*	*Tipus*	*Fi de vida*
Java	1.4.2_19		Tecnologia	ACABAT
Java	1.5.22		Tecnologia	ACABAT
Java	1.6.45		Tecnologia	ACABAT
Java	1.7.71		Tecnologia	ACABAT
.NET	4.5	Mono 4.2	Tecnologia	ACABAT

Glossari

PTN ELC: es tracta del Lloc de Treball Normalitzat amb Escriptori Lliure Corporatiu, és a dir, basat el sistema operatiu de desenvolupament propi de la Generalitat «Lliurex Admin» basat en Linux.

PTN EPC: es tracta del Lloc de Treball Normalitzat amb Escriptori Propietari Corporatiu, és a dir, basat en el sistema operatiu Microsoft Windows.

Remediacions: es tracta de programari i/o configuracions installades de manera excepcional que permeten l'execució d'aplicacions necessàries per als usuaris però que no s'han pogut actualitzar encara i no podrien funcionar sense aqueixes remediacions.

Fi de vida: si no ha acabat, es tracta de l'any en què finalitza el suport del producte per part del fabricant o del desenvolupador.

Tipus: el tipus de programari es correspon amb la classificació següent:

Tipus	*Descripció*
Ofimàtica	Programari per a generar i editar documents.
Internet	Programari per a mostrar pàgines web o realitzar altres tasques que requerisquen l'accés a internet.
Utilitat	Visors de documents, compressors, impressores virtuals, traductors, agendes, etc.
Infraestructura	Programari d'utilitat, gestió, control i seguretat de la DGTIC: antivirus, clients de gestió, clients d'accés, servidors d'accés, etc.
Multimèdia	Programari per a visionar o crear contingut multimèdia: fotos, vídeos i àudio.
Tecnologia	Connectors de navegadors, entorn de treball, llibreries. Programari intermediari en general.
Missatgeria	Programari per a llegir i crear correu, videoconferència i veu IP, missatges instantanis, etc.

ANNEX II

Política de contrasenyes en l'Administració de la GV

1. Introducció

El Decret 66/2012, de 27 d'abril, del Consell, pel qual s'estableix la política de seguretat de la informació de la Generalitat, en l'article 14 especifica que la política es desenvoluparà en un conjunt de documents l'objectiu del qual és facilitar que el tractament d'informació es realitze d'acord amb els objectius i principis exposats en aquesta. Que aquests documents estaran agrupats en tres col·leccions: normes, procediments i guies de bones pràctiques; que les normes proporcionaran un primer nivell de concreció, cada una d'aquestes estarà dirigida a un determinat tipus d'activitat; els procediments descriuran la seqüència concreta de passos per a completar una tasca, i les guies de bones pràctiques oferiran recomanacions sobre com actuar en situacions específiques. Que les normes i els procediments tindran caràcter obligatori i s'hauran de justificar les possibles excepcions.

L'Ordre 19/2013, de 3 de desembre, de la Conselleria d'Hisenda i Administració Pública, per la qual s'estableixen les normes sobre l'ús segur de mitjans tecnològics a l'Administració de la Generalitat, en l'article 7.4 estableix que 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.

Tecnología

Nombre software	*Versión en PTN EPC*	*Versión en PTN ELC*	*Tipo*	*Fin de Vida*
Java	1.4.2_19		Tecnología	ACABADO
Java	1.5.22		Tecnología	ACABADO
Java	1.6.45		Tecnología	ACABADO
Java	1.7.71		Tecnología	ACABADO
.NET	4.5	Mono 4.2	Tecnología	ACABADO

Glosario

– PTN ELC: se trata del Puesto de Trabajo Normalizado con Escritorio Libre Corporativo, es decir, basado el sistema operativo de desarrollo propio de la Generalitat «Lliurex Admin» basado en Linux.

– PTN EPC: se trata del Puesto de Trabajo Normalizado con Escritorio Propietario Corporativo, es decir, basado en el sistema operativo Microsoft Windows.

– Remediaciones: Se trata de *software* y/o configuraciones instaladas de manera excepcional que permiten la ejecución de aplicaciones necesarias para los usuarios pero que no se han podido actualizar todavía y no podrían funcionar sin esas remediaciones.

– Fin de vida: si no ha acabado, se trata del año en el que finaliza el soporte del producto por parte del fabricante o del desarrollador.

– Tipo: el tipo de *software* se corresponde con la clasificación siguiente:

Tipo	*Descripción*
Ofimática	Software para generar y editar documentos.
Internet	Software para mostrar páginas web o realizar otras tareas que requieran el acceso a internet.
Utilidad	Visores de documentos, compresores, impresoras virtuales, traductores, agendas, etc.
Infraestructura	Software de utilidad, gestión, control y seguridad de la DGTIC: antivirus, clientes de gestión, clientes de acceso, servidores de acceso, etc.
Multimedia	Software para visionar o crear contenido multimedia: fotos, vídeos y audio.
Tecnología	Plugins de navegadores, frameworks, librerías. Middleware en general.
Mensajería	Software para leer y crear correo, videoconferencia y voz ip, mensajes instantáneos, etc.

ANEXO II

Política de contraseñas en la Administración de la GV

1. Introducción

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 su artículo 14 especifica 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. Que estos documentos estarán agrupados en tres colecciones: normas, procedimientos y guías de buenas prácticas; que las normas proporcionarán un primer nivel de concreción, cada una de ellas estará dirigida a un determinado tipo de actividad; los procedimientos describirán la secuencia concreta de pasos para completar una tarea; y las guías de buenas prácticas ofrecerán recomendaciones sobre cómo actuar en situaciones específicas. Que las normas y los procedimientos tendrán carácter obligatorio, debiendo justificarse las posibles excepciones.

La Orden 19/2013, de 3 de diciembre, de la Conselleria de Hacienda y Administración Pública, por la que se establece las normas sobre el uso seguro de medios tecnológicos en la Administración de la Generalitat, en su artículo 7.4 establece que 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.

El Reial decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat en l'àmbit de l'Administració Electrònica, en l'annex II sobre les mesures de seguretat, estableix en l'apartat 4.2.5 que els mecanismes d'autenticació s'adequaran al nivell del sistema accedit. En concret, per als sistemes catalogats de nivell alt, no s'admetrà l'ús de claus concertades i s'exigirà l'ús de certificats digitals en dispositius físics personalitzats o biometria.

El Decret 130/2012, de 24 d'agost, del Consell, pel qual s'estableix l'organització de la seguretat de la informació de la Generalitat, en l'article 11 estableix que el responsable de seguretat de la informació té la responsabilitat de vetlar per la seguretat de la informació i dels serveis prestats pels sistemes d'informació, d'acord amb el que estableix la política de seguretat de la informació, i entre les seues funcions estan les funcions d'elaborar i aprovar els procediments operatius i les guies de bones pràctiques de seguretat de la informació. I en l'article 14 estableix que els administradors de la seguretat del sistema tenen la missió de la implementació, gestió i manteniment de les mesures de seguretat aplicables en el sistema d'informació i entre les seues funcions estan les d'assegurar que són aplicats els procediments aprovats per a manejar els sistemes d'informació i els mecanismes i serveis de seguretat requerits.

Es configura el present document com a Política de Contrasenyes a l'Administració de la Generalitat, que tindrà caràcter d'obligatori com a procediment operatiu. S'hi incorpora un apartat amb recomanacions sobre com actuar en situacions específiques que tindrà, a tots els efectes, la consideració de guia de bones pràctiques.

2. Objecte

L'objectiu fonamental d'aquest document és establir la Política de Contrasenyes a l'Administració de la Generalitat, la qual cosa inclou unes directrius sobre la selecció, ús i custòdia de contrasenyes, així com unes recomanacions sobre com actuar en situacions específiques.

3. Àmbit

L'àmbit d'aquesta política inclou tots aquells usuaris de les aplicacions, serveis i recursos informàtics que tenen o són responsables d'un compte (o qualsevol altre tipus d'accés que requerisca una contrasenya) en qualsevol dels sistemes corporatius de l'àmbit definit en el Decret 130/2012, de 24 d'agost, del Consell, pel qual s'estableix l'organització de la seguretat de la informació de la Generalitat.

4. Definicions

Contrasenya: informació d'autenticació confidencial, usualment composta per una cadena de caràcters.

Compte d'usuari: és aquell compte personal que dóna accés a aplicació, recurs o servei informàtic de la Generalitat (com per exemple compte del sistema operatiu, compte de correu, compte de servei web, etc.)

Compte d'administració: és aquell compte que dóna accés a aplicació, recurs o servei informàtic amb privilegis d'administració (com per exemple arrels, administradors Windows, comptes d'administració d'aplicacions, etc).

Compte instrumental d'aplicació: és aquell compte genèric que es crea per a interactuar entre aplicacions o dispositius (com per exemple compte definit en el servidor d'aplicacions per a connectar-se al SGBD).

5. Directrius

Totes les contrasenyes de comptes definides en l'apartat anterior que donen accés a sistemes d'informació de la Generalitat hauran de seguir les directrius assenyalades a continuació:

– Sempre que siga tècnicament possible, els sistemes o aplicacions es configuraran per a forçar que es complisquen les directrius indicades en aquest document. En tot cas, persisteix l'obligació de l'usuari a complir-les.

– Els comptes d'administració han de tindre contrasenyes distintes entre si i diferents de la resta de comptes mantinguts pel dit usuari.

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, en su anexo II sobre las medidas de seguridad, establece en su apartado 4.2.5 que los mecanismos de autenticación, se adecuarán al nivel del sistema accedido. En concreto, para los sistemas catalogados de nivel alto, no se admitirá el uso de claves concertadas y se exigirá el uso de certificados digitales en dispositivos físicos personalizados o biometría.

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, en su artículo 11 establece que el Responsable de Seguridad de la Información tiene la responsabilidad de velar por la seguridad de la información y de los servicios prestados por los sistemas de información, de acuerdo a lo establecido en la Política de Seguridad de la Información, y entre sus funciones están las de elaborar y aprobar los procedimientos operativos y las guías de buenas prácticas de seguridad de la información. Y En su artículo 14 establece que los Administradores de la Seguridad del Sistema tienen la misión de la implementación, gestión y mantenimiento de las medidas de seguridad aplicables en el sistema de información, y entre sus funciones están las de asegurar que son aplicados los procedimientos aprobados para manejar los sistemas de información y los mecanismos y servicios de seguridad requeridos.

Se configura el presente documento como Política de Contraseñas en la Administración de la Generalitat, que tendrá carácter de obligatorio como procedimiento operativo. Se incorpora un apartado con recomendaciones sobre cómo actuar en situaciones específicas que tendrá a todos los efectos consideración de guía de buenas prácticas.

2. Objeto

El objetivo fundamental de este documento es establecer la Política de Contraseñas en la Administración de la Generalitat, lo que incluye unas directrices sobre la selección, uso y custodia de contraseñas, así como unas recomendaciones sobre cómo actuar en situaciones específicas.

3. Ámbito

El ámbito de esta política incluye a todos aquellos usuarios de las aplicaciones, servicios y recursos informáticos que tienen o son responsables de una cuenta (o cualquier otro tipo de acceso que requiera una contraseña) en cualquiera de los sistemas corporativos del ámbito definido 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.

4. Definiciones

Contraseña: Información de autenticación confidencial, usualmente compuesta por una cadena de caracteres.

Cuenta de usuario: Es aquella cuenta personal que da acceso a aplicación, recurso o servicio informático de la Generalitat (como por ejemplo cuenta del sistema operativo, cuenta de correo, cuenta de servicio web, etc).

Cuenta de administración: Es aquella cuenta que da acceso a aplicación, recurso o servicio informático con privilegios de administración (como por ejemplo root, administradores Windows, cuentas de administración de aplicaciones, etc).

Cuenta instrumental de aplicación: Es aquella cuenta genérica que se crea para interactuar entre aplicaciones o dispositivos.(Como por ejemplo cuenta definida en el servidor de aplicaciones para conectarse al SGBD).

5. Directrices

Todas las contraseñas de cuentas definidas en el apartado anterior que den acceso a sistemas de información de la Generalitat deberán seguir las directrices señaladas a continuación:

– Siempre que sea técnicamente posible, los sistemas o aplicaciones se configurarán para forzar que se cumplan las directrices indicadas en este documento. En cualquier caso, persiste la obligación del usuario a cumplirlas.

– Las cuentas de administración, deben tener contraseñas distintas entre ellas y diferentes del resto de cuentas mantenidas por dicho usuario.

– Les contrasenyes per defecte associades als sistemes o aplicacions hauran de ser canviades abans de posar aquests sistemes en producció.

– Algunes aplicacions, recursos o serveis informàtics en què siga especialment crític mantindre la seguretat de la contrasenya podran determinar-se mesures més restrictives de protecció d'aquesta.

5.1. Morfologia

Les contrasenyes hauran de complir les especificacions que es defineixen a continuació:

– Han de tindre una longitud mínima de 8 caràcters.

– Han d'incloure caràcters com a mínim de tres de les categories següents: majúscules, minúscules, números i caràcters no alfanumèrics, com a signes de puntuació i símbols.

– No ha de contindre el nom del compte de l'usuari, l'adreça electrònica o parts del nom de l'usuari.

– No es pot repetir cap de les 5 contrasenyes anteriors que s'hagen usat.

5.2. Bloqueig

S'aplicarà el sistema de bloqueig d'accés que s'indica a continuació:

– Quan un usuari introduïsca 5 vegades seguides una contrasenya errònia, l'accés d'aqueix usuari quedarà bloquejat provisionalment.

– Es podran establir mecanismes en què el mateix usuari puga desbloquejar el seu compte, sempre que puga identificar-se a través d'un certificat digital vàlid.

– No s'establirà cap mecanisme de desbloqueig automàtic de comptes, pel mer fet de transcórrer un cert espai de temps.

5.3. Canvi

S'aplicarà el sistema de canvi obligatori de contrasenya que s'indica a continuació:

– Els comptes d'usuari hauran de canviar la contrasenya almenys cada 3 mesos.

– Els comptes instrumentals d'aplicació i les d'administració s'han de canviar anualment.

– El sistema recordarà a l'usuari que ha de canviar la contrasenya 10 dies abans que caduque.

– Si en acabar el termini no s'ha fet el canvi, el sistema sol·licitarà el canvi obligatòriament.

– No podrà canviar-se abans de dos dies.

5.4. Lliurament i custòdia

– El lliurament de les contrasenyes inicials es realitzarà per mitjans que n'eviten la intercepció i que al seu torn permeten verificar-ne la identitat del receptor.

– Les contrasenyes inicials seran generades automàticament amb les característiques recomanades en aquesta política i es trobaran en estat expirat, per a obligar l'usuari a canviar-la en el primer ús que facen del compte.

– Per a donar validesa a la seua contrasenya l'usuari haurà de fer una acceptació expressa d'aquesta política de contrasenyes. Des d'aqueix moment és responsabilitat de l'usuari mantindre en secret la dita clau.

– No s'ha de compartir ni revelar els comptes i contrasenyes amb ningú, totes les contrasenyes han de ser tractades com informació sensible i confidencial, fins i tot encara que li parlen en nom de la DGTI o d'un superior seu en l'organització.

– L'emmagatzematge de les contrasenyes en els sistemes d'autenticació ha de realitzar-se de manera xifrada perquè es garantisca la confidencialitat d'aquesta i que ningú, excepte l'usuari, tinga el control sobre aquesta.

– No s'ha d'utilitzar la característica de «Recordar Contrasenya» existent en algunes aplicacions.

– S'establiran auditories sobre el canvi de contrasenyes per a detectar i controlar qualsevol incidència que puga afectar l'accés d'un compte.

5.5. Inactivitat

– Els comptes d'usuari es bloquejaran després d'una inactivitat de 3 mesos.

– Per als comptes de nova creació, el període d'inactivitat serà de 15 dies.

6. Recomanacions

6.1. Recomanacions generals per a la selecció de contrasenyes

– Las contraseñas por defecto asociadas a los sistemas o aplicaciones deberán ser cambiadas antes de poner estos sistemas en producción.

– Algunas aplicaciones, recursos o servicios informáticos en los que sea especialmente crítico mantener la seguridad de la contraseña podrán determinarse medidas más restrictivas de protección de la misma.

5.1. Morfología

Las contraseñas deberán cumplir con las especificaciones que se definen a continuación:

– Deben tener una longitud mínima de 8 caracteres.

– Deben incluir caracteres de al menos tres de las siguientes categorías: mayúsculas, minúsculas, números y caracteres no alfanuméricos, como signos de puntuación y símbolos.

– No debe contener el nombre de la cuenta del usuario, el email, o partes del nombre del usuario.

– No se puede repetir ninguna de las 5 contraseñas anteriores que se hayan usado.

5.2. Bloqueo

Se aplicará el sistema de bloqueo de acceso que se indica a continuación:

– Cuando un usuario introduzca 5 veces seguidas una contraseña errónea, el acceso de ese usuario quedará bloqueado provisionalmente.

– Se prodrán establecer mecanismos en los que el propio usuario pueda desbloquear su cuenta, siempre que pueda identificarse a través de un certificado digital válido.

– No se establecerá ningún mecanismo de desbloqueo automático de cuentas, por el mero hecho de transcurrir un cierto lapso de tiempo.

5.3. Cambio

Se aplicará el sistema de cambio obligatorio de contraseña que se indica a continuación:

– Las cuentas de usuario deberán cambiar la contraseña al menos cada 3 meses.

– Las cuentas instrumentales de aplicación y las de administración se han de cambiar anualmente.

– El sistema recordará al usuario que debe cambiar la contraseña 10 días antes de que caduque.

– Si al terminar el plazo no se ha hecho el cambio, el sistema solicitará su cambio obligatoriamente.

– No podrá cambiarse antes de dos días.

5.4. Entrega y custodia

– La entrega de las contraseñas iniciales se realizará por medios que eviten la interceptación y que a su vez permitan verificar la identidad del receptor.

– Las contraseñas iniciales serán generadas automáticamente con las características recomendadas en esta política, y se encontrarán en estado expirado, para obligar al usuario a cambiarla en el primer uso que hagan de la cuenta.

– Para dar validez a su contraseña el usuario tendrá que hacer una aceptación expresa de esta política de contraseñas. Desde ese momento es responsabilidad del usuario mantener en secreto dicha clave.

– No se debe compartir ni revelar las cuentas y contraseñas con nadie, todas las contraseñas deben ser tratadas como información sensible y confidencial, incluso aunque le hablen en nombre de la DGTI, o de un superior suyo en la organización.

– El almacenamiento de las contraseñas en los sistemas de autenticación debe realizarse de manera cifrada para que se garantice la confidencialidad de la misma y que nadie, excepto el usuario tenga el control sobre ella.

– No utilizar la característica de «Recordar Contraseña» existente en algunas aplicaciones.

– Se establecerán auditorias sobre el cambio de contraseñas para detectar y controlar cualquier incidencia que pueda afectar al acceso de una cuenta.

5.5. Inactividad

– Las cuentas de usuario se bloquearán tras una inactividad de 3 meses.

– Para las cuentas de nueva creación, el periodo de inactividad será de 15 días.

6. Recomendaciones

6.1. Recomendaciones generales para la selección de contraseñas

La seguretat de l'autenticació amb contrasenya es basa en la premissa que la contrasenya és suficient robusta per a no ser desxifrada fàcilment.

Una contrasenya «robusta» (segura) és una cadena de caràcters que té les següents característiques:

– Té una longitud mínima de 8 caràcters.

– No es troba en el diccionari (espanyol o estranger).

– No pot derivar-se d'informació personal de l'usuari:

– Data de naixement,

– Adreça o telèfon,

– DNI,

– Noms de familiars, animals, companys de treball, amics o personatges de ficció.

– No és d'ús comú, com per exemple:

– Termes i marques informàtics, comandaments, companyies comercials, maquinari, programari.

– Patrons de lletres o números, com ara 'aaabbb', 'qwerty', 'zxywvu', '123321′, …

– Qualsevol de l'anterior escrit al revés.

– Qualsevol de l'anterior precedit o seguit per un dígit, per exemple 'secret1′ o '1secret'.

S'intentaran crear contrasenyes que es puguen recordar fàcilment. Una senzilla forma de recordar-la és crear una contrasenya basada en una frase recordable amb facilitat.

6.2. Recomanacions per a la protecció de la contrasenya

A continuació es presenta una llista de recomanacions:

– No ha d'utilitzar-se la mateixa contrasenya que s'utilitza per a altres comptes externs a l'organització.

– No revelar la contrasenya en missatges de correu electrònic ni a través de qualsevol altre mitjà de comunicació electrònica. Si algú li sol·licita la contrasenya, faça referència a aquest document.

– Mai escriure la contrasenya en paper ni emmagatzemar-la en fitxers d'ordinador sense xifrar o desproveït d'algun mecanisme de seguretat.

– No revelar la contrasenya en cap qüestionari o formulari, independentment de la confiança que inspire aquest.

– Davant de la menor sospita que algun dels seus comptes o les seues contrasenyes puguen haver sigut compromeses, ha de tractar açò com un incident de seguretat, comunicar-ho per les vies establides per a això i hauria de canviar les contrasenyes de tots els seus comptes.

– En cap concepte, se sol·licita als usuaris que introduïsquen les seues credencials per a 'validació' en llocs de tercers ni en correus electrònics, per la qual cosa qualsevol correu en què se li sol·licite introduir aquest tipus d'informació serà fraudulent.

La seguridad de la autenticación con contraseña se basa en la premisa de que la contraseña es lo suficientemente robusta para no ser descifrada fácilmente.

Una contraseña «robusta» (segura) es una cadena de caracteres que tiene las siguientes características:

– Tiene una longitud mínima de 8 caracteres.

– No se encuentra en el diccionario (español o extranjero).

– No puede derivarse de información personal del usuario:

– Fecha de nacimiento,

– Dirección o teléfono,

– DNI,

– Nombres de familiares, animales, compañeros de trabajo, amigos o personajes de ficción.

– No es de uso común, como por ejemplo:

– Términos y marcas informáticos, comandos, compañías comerciales, *hardware*, *software*.

– Patrones de letras o números, como 'aaabbb',' qwerty',' zxywvu', '123321′, …

– Cualquiera de lo anterior escrito al revés.

– Cualquiera de lo anterior precedido o seguido por un dígito, por ejemplo 'secreto1′ o '1secreto'.

Se intentarán crear contraseñas que se puedan recordar fácilmente. Una sencilla forma de recordarla es crear una contraseña basada en una frase recordable con facilidad.

6.2. Recomendaciones para la protección de la contraseña

A continuación se presenta una lista de recomendaciones:

– No debe utilizarse la misma contraseña que se utiliza para otras cuentas externas a la organización.

– No revelar la contraseña en mensajes de correo electrónico ni a través de cualquier otro medio de comunicación electrónica. Si alguien le solicita la contraseña, refiérale a este documento.

– Nunca escribir la contraseña en papel ni almacenarla en ficheros de ordenador sin cifrar o desprovisto de algún mecanismo de seguridad.

– No revelar la contraseña en ningún cuestionario o formulario, independientemente de la confianza que inspire el mismo.

– Ante la menor sospecha de que alguna de sus cuentas o sus contraseñas puedan haber sido comprometidas, debe tratar esto como un incidente de seguridad, comunicarlo por los cauces establecidos para ello y debería cambiar las contraseñas de todas sus cuentas.

– Bajo ningún concepto, se solicita a los usuarios que introduzcan sus credenciales para «validación» en sitios de terceros ni en correos electrónicos, por lo que cualquier correo en el que se le solicite introducir este tipo de información será fraudulento.