La Comissió Interdepartamental estarà formada pels següents membres:

– President o presidenta: el conseller o consellera de Justícia i Administracions Públiques.

– Vicepresident o vicepresidenta: el director o directora general de Justícia.

– Secretari o secretària: el subsecretari o subsecretària del Secretariat del Govern i Relacions amb les Corts.

– Vocals:

· Un representant de la Conselleria de Cultura, Educació i Ciència, amb rang de director o directora general o equivalent, nomenat pel conseller o consellera del departament.

· Un representant de la Conselleria d'Indústria i Comerç, amb rang de director o directora general o equivalent, nomenat pel conseller o consellera del departament.

· Un representant de la Conselleria d'Agricultura, Pesca i Alimentació, amb rang de director o directora general o equivalent, nomenat pel conseller o consellera del departament.

· Un representant de la Conselleria de Medi Ambient, amb rang de director o directora general o equivalent, nomenat pel conseller o consellera del departament.

· Un representant de la Conselleria d'Economia i Hisenda, amb rang de director o directora general o equivalent, nomenat pel conseller o consellera del departament.

L'Àrea del Gabinet de Coordinació Interdepartamental de la Presidència exercirà la secretaria administrativa de la Comissió».

DISPOSICIONS FINALS

Primera

Es faculta el conseller o consellera de Justícia i Administracions Públiques per a dictar totes les disposicions que resulten necessàries per al desplegament, execució i compliment d'allò que s'ha disposat en el present decret.

Segona

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

València, 11 de gener de 2000

El president de la Generalitat Valenciana,
EDUARDO ZAPLANA HERNÁNDEZ-SORO

El conseller de Justícia i Administracions Públiques,
SERAFÍN CASTELLANO GÓMEZ

ORDRE de 3 de desembre de 1999, de la Conselleria de Justícia i Administracions Públiques, per la qual s'aprova el Reglament Tècnic de Mesures de Seguretat per a l'Aprovació i Homologació d'Aplicacions i Mitjans de Tractament Automatitzat de la Informació. [1999/M11020]

La introducció de les noves tecnologies del tractament de la informació ha suposat un notable avanç en els processos de racionalització i modernització de les administracions públiques. Tot i això, la seua utilització requereix l'establiment d'uns requisits que garantisquen els drets dels ciutadans.

En l'article 45 de la Llei 30/1992, de 26 de novembre, de Règim Jurídic de les Administracions Públiques i del Procediment Administratiu Comú, es consagra la utilització dels mitjans electrònics, informàtics i telemàtics per part de les unitats administratives, per a l'exercici de les seues competències. En aquest article es regulen els requisits bàsics que han de complir aquests mitjans, a fi que els seus resultats gaudisquen de validesa jurídica plena.

Addicionalment, la Generalitat Valenciana ha efectuat un desplegament normatiu d'aquest article plasmat en el Decret 96/1998,

La Comisión Interdepartamental estará formada por los siguientes miembros:

– Presidente o presidenta: el conseller o consellera de Justicia y Administraciones Públicas.

– Vicepresidente o vicepresidenta: el director o directora general de Justicia.

– Secretario o secretaria: El subsecretario o subsecretaria del Secretariado del Gobierno y Relaciones con las Cortes.

– Vocales:

· Un representante de la Conselleria de Cultura, Educación y Ciencia, con rango de director o directora general o equivalente, nombrado por el conseller o consellera del departamento.

· Un representante de la Conselleria de Industria y Comercio, con rango de director o directora general o equivalente, nombrado por el conseller o consellera del departamento.

· Un representante de la Conselleria de Agricultura, Pesca y Alimentación, con rango de director o directora general o equivalente, nombrado por el conseller o consellera del departamento.

· Un representante de la Conselleria de Medio Ambiente, con rango de director o directora general o equivalente, nombrado por el conseller o consellera del departamento.

· Un representante de la Conselleria de Economía y Hacienda, con rango de director o directora general o equivalente, nombrado por el conseller o consellera del departamento.

El Área del Gabinete de Coordinación Interdepartamental de la Presidencia desempeñará la Secretaría Administrativa de la Comisión».

DISPOSICIONES FINALES

Primera

Se faculta al conseller o consellera de Justicia y Administraciones Públicas a dictar cuantas disposiciones resulten necesarias para el desarrollo, ejecución y cumplimiento de lo dispuesto en el presente decreto.

Segunda

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

Valencia, 11 de enero de 2000

El presidente de la Generalitat Valenciana,
EDUARDO ZAPLANA HERNÁNDEZ-SORO

El conseller de Justicia y Administraciones Públicas,
SERAFÍN CASTELLANO GÓMEZ

ORDEN de 3 de diciembre de 1999, de la Conselleria de Justicia y Administraciones Públicas, por la que se aprueba el Reglamento Técnico de Medidas de Seguridad para la Aprobación y Homologación de Aplicaciones y Medios de Tratamiento Automatizado de la Información. [1999/M11020]

La introducción de las nuevas tecnologías del tratamiento de la información ha supuesto un notable avance en los procesos de racionalización y modernización de las administraciones públicas. Sin embargo, su utilización requiere el establecimiento de unos requisitos que garanticen los derechos de los ciudadanos.

En el artículo 45 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, se consagra la utilización de los medios electrónicos, informáticos y telemáticos por parte de las unidades administrativas para el ejercicio de sus competencias. En este artículo se regulan los requisitos básicos que deben cumplir estos medios con la finalidad de que sus resultados gocen de validez jurídica plena.

Adicionalmente, la Generalitat Valenciana ha efectuado un desarrollo normativo de este artículo plasmado en el Decreto

de 6 de juliol, pel qual es regula, entre altres, la utilització de les tècniques electròniques, informàtiques i telemàtiques. En aquest decret es fixen les aplicacions sotmeses a aprovació, es detallen els requeriments a cobrir per cadascun dels elements implicats en el tractament de la informació i es dicta el procediment mitjançant el qual un sistema és aprovat i publicat.

Tanmateix, i atesos els criteris fixats en el Decret 96/1998, de 6 de juliol, no es pot arribar al nivell de detall necessari per a reformar les garanties estipulades en aquest, i en diferents articles s'estableix l'obligació d'efectuar un desplegament reglamentari que proporcione l'adequat nivell de concreció als requisits que de forma general s'estableixen en el decret.

Addicionalment, i donat que la gestió dels documents electrònics no es troba totalment resolta, i per tant normalitzada en les aplicacions d'utilització general, procedeix efectuar un desplegament específic, a fi de contemplar la casuística particular del tractament documental.

Per tant, es fa convenient dictar una normativa de desplegament que establisca reglamentàriament, de mode unificat i al nivell de detall necessari, quins són els requisits tècnics i d'organització que proporcionen les garanties estipulades per a la utilització dels mitjans electrònics, informàtics i telemàtics, incloent la gestió dels documents.

La disposició final del Decret 96/1998, de 6 de juliol, autoritza el conseller d'Economia, Hisenda i Administració Pública per a dictar totes les disposicions que siguen calguen per a establir criteris generals en desplegament i execució d'allò que disposat aquest, previ informe de Comité Tècnic per al Desplegament dels Sistemes d'Informació.

Així mateix, l'Ordre de 29 de setembre de 1999, de la Conselleria de Justícia i Administracions Públiques, per la qual es desplega el Decret 91/1999, de 30 de juliol, del Govern Valencià, amb què s'aprova el Reglament Orgànic i Funcional de la Conselleria de Justícia i Administracions Públiques, estableix en el seu article 6:

«La Direcció General per a la Modernització i Racionalització de l'administració Pública, desplega les funcions derivades de les competències previstes en l'article 16 del Reglament Orgànic i Funcional i aquelles altres, excepte les relatives a matèria de personal, atribuïdes a la Subsecretaria per a la Modernització de les Administracions Públiques i a l'anterior Direcció General per a la Racionalització del Sector Públic en les altres disposicions normatives; així mateix, les referències en les mateixes al conseller d'Economia, Hisenda i Administració Pública s'entendran fetes al conseller de Justícia i Administracions Públiques.»

En la seua virtut, i en exercici de les competències que em confereix l'article 35 de la Llei 5/1983, de 30 de desembre, de Govern Valencià

DISPOSE

Article únic

S'aprova el Reglament Tècnic d'Aprovació i Homologació d'Aplicacions i Mitjans de Tractament Automatitzat de la Informació, que figura com annex a la present ordre.

DISPOSICIÓ TRANSITÒRIA

Adequació de suports, mitjans i aplicacions.

Sense perjudici d'allò establit en la normativa estatal, totes les aplicacions aprovades amb anterioritat a la data de publicació de la present disposició disposaran d'un any per a adaptar-se als preceptes del reglament.

No obstant això, per a aquelles aplicacions que tecnològicament no puguen complir algun dels requisits expressats en el present reglament, l'autoritat d'autentificació, i de forma motivada per l'organisme responsable de l'aplicació, i en l'exercici de les funcions reconegudes en l'article 20.b) del Decret 96/1998, de 6 de juliol, podrà ampliar el seu termini d'adaptació en funció de la seua complexitat tècnica, fins a un màxim de tres anys.

96/1998, de 6 de julio, por el que se regula, entre otros, la utilización de las técnicas electrónicas, informáticas y telemáticas. En este decreto se fijan las aplicaciones sometidas a aprobación, se detallan los requerimientos a cubrir por cada uno de los elementos implicados en el tratamiento de la información y se dicta el procedimiento mediante el cual un sistema es aprobado y publicado.

Sin embargo, dado que los criterios fijados en el Decreto 96/1998, de 6 de julio, no pueden llegar al nivel de detalle necesario para afianzar las garantías estipuladas en el mismo, en diferentes artículos se establece la obligación de efectuar un desarrollo reglamentario que proporcione el adecuado nivel de concreción a los requisitos que de forma general se establecen en el decreto.

Adicionalmente, dado que la gestión de los documentos electrónicos no se encuentra totalmente resuelta, y por tanto normada, en las aplicaciones de utilización general, procede efectuar un desarrollo específico con el fin de contemplar la casuística particular del tratamiento documental.

Se hace, pues, de todo punto conveniente dictar una normativa de desarrollo que establezca reglamentariamente, de modo unificado y al nivel de detalle necesario, cuales son los requisitos técnicos y de organización que proporcionan las garantías estipuladas para la utilización de los medios electrónicos, informáticos y telemáticos, incluyendo la gestión de los documentos.

La Disposición Final del Decreto 96/1998, de 6 de julio, autoriza al conseller de Economía, Hacienda y Administración Pública para dictar cuantas disposiciones sean precisas para establecer criterios generales en desarrollo y ejecución de lo dispuesto en el mismo, previo informe de Comité Técnico para el Desarrollo de los Sistemas de Información.

Asimismo, la Orden de 29 de septiembre de 1999, de la Conselleria de Justicia y Administraciones Públicas, por la que se desarrolla el Decreto 91/1999, de 30 de julio, del Gobierno Valenciano, por el que se aprueba el Reglamento Orgánico y Funcional de la Conselleria de Justicia y Administraciones Públicas, establece en su artículo 6 :

«La Dirección General para la Modernización y Racionalización de la Administración Pública, desarrolla las funciones derivadas de las competencias previstas en el artículo 16 del Reglamento Orgánico y Funcional y aquellas otras, salvo las relativas a materia de personal, atribuidas a la Subsecretaría para la Modernización de las Administraciones Públicas y a la anterior Dirección General para la Racionalización del Sector Público en las demás disposiciones normativas, asimismo, las referencias en las mismas al conseller de Economía, Hacienda y Administración Pública se entenderán hechas al conseller de Justicia y Administraciones Públicas.»

En su virtud, y en ejercicio de las competencias que me confiere el artículo 35 de la Ley 5/1983, de 30 de diciembre, de Gobierno Valenciano

DISPONGO

Artículo único

Se aprueba el Reglamento Técnico de Aprobación y Homologación de Aplicaciones y Medios de Tratamiento Automatizado de la Información, que figura como anexo a la presente orden.

DISPOSICIÓN TRANSITORIA

Adecuación de soportes, medios y aplicaciones.

Sin perjuicio de lo establecido en la normativa estatal, todas las aplicaciones aprobadas con anterioridad a la fecha de publicación de la presente disposición dispondrán de un año para adaptarse a los preceptos del reglamento.

No obstante, para aquellas aplicaciones que tecnológicamente no puedan cumplir alguno de los requisitos expresados en el presente reglamento, la autoridad de autentificación, de forma motivada por el organismo responsable de la aplicación, y en el ejercicio de las funciones reconocidas en el artículo 20.b) del Decreto 96/1998, de 6 de julio, podrá ampliar su plazo de adaptación en función de su complejidad técnica, hasta un máximo de tres años.

DISPOSICIONS FINALS

Primera. Desplegament del reglament

S'autoritza la directora general per a la Modernització i Racionalització de l'administració Pública per a dictar les instruccions oportunes en ordre a la interpretació i aplicació del reglament.

Segona. Entrada en vigor

La present ordre entrarà en vigor al mes de la seua publicació en el *Diari Oficial de la Generalitat Valenciana.*

València, 3 de desembre de 1999

El conseller de Justícia i Administracions Públiques,
SERAFÍN CASTELLANO GÓMEZ

ANNEX

Reglament Tècnic de Mesures de Seguretat per a l'Aprovació i Homologació d'Aplicacions i Mitjans de Tractament Automatitzat de la Informació

Índex

DISPOSICIONES FINALES

Primera. Desarrollo del reglamento

Se autoriza a la directora general para la Modernización y Racionalización de la Administración Pública para dictar las instrucciones oportunas en orden a la interpretación y aplicación del reglamento.

Segunda. Entrada en vigor.

La presente orden entrará en vigor al mes de su publicación en el *Diari Oficial de la Generalitat Valenciana.*

Valencia, 3 de diciembre de 1999

El conseller de Justicia y Administraciones Públicas,
SERAFÍN CASTELLANO GÓMEZ

ANEXO

Reglamento Técnico de Medidas de Seguridad para la Aprobación y Homologación de Aplicaciones y Medios de Tratamiento Automatizado de la Información

Índice

TÍTOL I
Disposicions generals

Article 1. Objecte

El present reglament té per objecte la regulació, en l'àmbit de la Generalitat Valenciana, de les mesures de seguretat i organització que han de reunir les aplicacions electròniques, informàtiques o telemàtiques, com també el tractament dels documents electrònics en aquestes aplicacions.

Article 2. Àmbit d'aplicació

1. Aquest reglament serà d'aplicació a totes les aplicacions sotmeses al procediment d'aprovació, publicació i homologació establit en el Decret 96/1998, de 6 de juliol, pel qual es regula, entre altres aspectes, la utilització dels sistemes d'informació.

Article 3. Definicions

a) Usuari: subjecte o procés que utilitza una aplicació.

b) Codi d'usuari: codi que l'aplicació utilitza per a identificar un usuari.

c) Contrasenya o clau: informació confidencial, freqüentment constituïda per una cadena de caràcters, que s'utilitza per a l'autentificació d'un usuari.

d) Permisos: nivell de seguretat que proporciona una determinada clau.

e) Clau amb privilegis d'accés: aquelles claus que permeten canviar certs controls de seguretat de l'aplicació.

f) Clau compartida o multiusuari: aquella clau que permet a un grup d'usuaris utilitzar concurrentment l'aplicació usant una mateixa clau.

g) Porta falsa: aquella clau secreta, no registrada en l'aplicació, però que permet superar, total o parcialment, els mecanismes de seguretat del sistema d'informació.

h) Tercera part: persona física o jurídica distinta de l'administració de la Generalitat Valenciana.

i) Sistema de tallafocs: sistema que restringeix i filtra l'accés, efectuat per mitjos telemàtics, a les aplicacions.

TÍTULO I
Disposiciones generales

Artículo 1. Objeto

El presente reglamento tiene por objeto la regulación, en el ámbito de la Generalitat Valenciana, de las medidas de seguridad y organización que deben reunir las aplicaciones electrónicas, informáticas o telemáticas así como el tratamiento de los documentos electrónicos en estas aplicaciones.

Artículo 2. Ámbito de aplicación

1. Este reglamento será de aplicación a todas las aplicaciones sometidas al procedimiento de aprobación, publicación y homologación establecido en el Decreto 96/1998, de 6 de julio, por el que se regula, entre otros aspectos, la utilización de los sistemas de información.

Artículo 3. Definiciones

a) Usuario: sujeto o proceso que utiliza una aplicación

b) Código de usuario: código que la aplicación utiliza para identificar un usuario

c) Contraseña o clave: información confidencial, frecuentemente constituida por una cadena de caracteres, que se utiliza para la autenticación de un usuario

d) Permisos: nivel de seguridad que proporciona una determinada clave

e) Clave con privilegios de acceso: aquellas claves que permiten cambiar ciertos controles de seguridad de la aplicación.

f) Clave compartida o multiusuario: aquella clave que permite a un grupo de usuarios utilizar concurrentemente la aplicación usando una misma clave

g) Puerta falsa: aquella clave secreta, no registrada en la aplicación, pero que permite superar, total o parcialmente, los mecanismos de seguridad del sistema de información.

h) Tercera parte: persona física o jurídica distinta de la administración de la Generalitat Valenciana

i) Sistema de cortafuegos: sistema que restringe y filtra el acceso, efectuado por medios telemáticos, a las aplicaciones.

j) Contingència: tota aquella situació que supose una alteració de les condicions normals d'explotació de l'aplicació. Inclou des de caigudes de tensió fins a danys irreparables en unitats d'emmagatzemament, passant per saturació de línies de comunicacions

k) Procés informàtic: programa o conjunt de programes informàtics pertanyents a una aplicació, que produeixen un resultat concret.

l) Sistema operatiu: programa o conjunt de programes informàtics de nivell bàsic, que permeten la interacció entre els equips físics i les aplicacions.

m) Servidor d'aplicació: tots els sistemes, equips i mitjans que suporten l'execució d'una aplicació, sempre que la seua arquitectura permeta la utilització simultània per més d'un usuari.

n) Virus informàtic: programa informàtic la finalitat del qual consisteix en alguna de les següents funcions:

– Alterar el funcionament dels equips.

– Destruir la informació existent en els suports d'emmagatzemament.

ñ) Salvament: operació consistent en extraure una còpia de les dades actuals d'una aplicació, des del dispositiu d'emmagatzemament habitual a un altre dispositiu diferent, al fi de garantir la conservació de la informació.

o) Compactació: procés mitjançant el qual s'eliminen aquelles dades no essencials de l'aplicació. És un procés que s'executa amb la finalitat d'estalviar espai d'emmagatzemament. La informació compactada pot mantenir-se en l'equip o bé pot ser salvada i eliminada d'aquest.

p) Tipus de documents electrònics: s'entén cadascun dels distints tipus de documents que intervenen en un expedient individual. Per tant, la distinció és funcional per la seua naturalesa administrativa, no pel seu format electrònic.

q) Alteració de documents: s'entén que un document electrònic és alterat quan es canvia el contingut d'aquest, és a dir, quan es canvia aquell que substancia l'acte administratiu, sense perjudici que tecnològicament puguen modificar-se alguns atributs de l'entitat electrònica que suporta el contingut del mateix, atributs que no afecten el contingut jurídic del document.

TÍTOL II
Mesures tècniques de seguretat i conservació de les aplicacions

CAPÍTOL I
Seguretat de les aplicacions

Article 4. Xifrat

1. Els algoritmes de xifrat que s'empren per a garantir l'autenticitat, integritat i confidencialitat de les informacions, així com de les seues transmissions, hauran de basar-se, quan tecnològicament es troben contemplades, en normes establides per AENOR o per algun dels organismes reconeguts per aquest organisme nacional.

2. Quan no puga emprar una normativa establida per AENOR, o per algun dels organismes reconeguts per aquest organisme nacional, l'autoritat autentificadora aprovarà l'algoritme de xifrat empleat.

3. Els algoritmes de xifrat utilitzats per l'aplicació han de ser publicats juntament amb les característiques d'aquesta.

Article 5. Ús del control d'accés

Per a poder usar una aplicació caldrà introduir o teclejar, si més no, la contrasenya que l'usuari posseïsca, sense perjudici de la utilització d'altres mecanismes addicionals que incrementen el nivell de seguretat de l'aplicació.

Article 6. Control d'accés. Accessos especials i vigència d'accessos

1. L'aplicació no ha de permetre la utilització de claus compartides o multiusuaris, per tant la clau ha de ser un identificador únic, personal i intransferible de l'usuari.

j) Contingencia: toda aquella situación que suponga una alteración de las condiciones normales de explotación de la aplicación. Incluye desde caídas de tensión hasta daños irreparables en unidades de almacenamiento pasando por saturación de líneas de comunicaciones

k) Proceso informático: programa o conjunto de programas informáticos pertenecientes a una aplicación que producen un resultado concreto.

l) Sistema operativo: programa o conjunto de programas informáticos de nivel básico que permiten la interacción entre los equipos físicos y las aplicaciones.

m) Servidor de aplicación: todos los sistemas, equipos y medios que soportan la ejecución de una aplicación, siempre que su arquitectura permita su utilización simultánea por mas de un usuario.

n) Virus informático: programa informático cuya finalidad consiste en alguna de las siguientes:

– Alterar el funcionamiento de los equipos

– Destruir la información existente en los soportes de almacenamiento

ñ) Salvado: operación consistente en extraer una copia de los datos actuales de una aplicación desde el dispositivo de almacenamiento habitual a otro dispositivo diferente con el fin de garantizar la conservación de la información

o) Compactación: proceso mediante el cual se eliminan aquellos datos no esenciales de la aplicación. Es un proceso que se ejecuta con el fin de ahorrar espacio de almacenamiento. La información compactada puede mantenerse en el equipo o bien puede ser salvada y eliminada del mismo.

p) Tipos de documentos electrónicos: Se entiende cada uno de los distintos tipos de documentos que intervienen en un expediente individual. Por tanto, la distinción es funcional, por su naturaleza administrativa, no por su formato electrónico.

q) Alteración de documentos: Se entiende que un documento electrónico es alterado cuando se cambia el contenido del mismo, aquel que sustancia el acto administrativo, sin perjuicio de que tecnológicamente puedan modificarse algunos atributos de la entidad electrónica que soporta el contenido del mismo, atributos que no afectan al contenido jurídico del documento.

TÍTULO II
Medidas técnicas de seguridad y conservación de las aplicaciones

CAPÍTULO I
Seguridad de las aplicaciones

Artículo 4. Cifrado

1. Los algoritmos de cifrado que se empleen para garantizar la autenticidad, integridad y confidencialidad de las informaciones, así como de sus transmisiones, deberán basarse, cuando tecnológicamente se encuentren contempladas, en normas establecidas por AENOR o por alguno de los organismos reconocidos por este organismo nacional.

2. Cuando no pueda emplearse una normativa establecida por AENOR, o por alguno de los organismos reconocidos por este organismo nacional, la autoridad autentificadora aprobará el algoritmo de cifrado empleado.

3. Los algoritmos de cifrado utilizados por la aplicación deben ser publicados junto con las características de la misma.

Artículo 5. Uso del control de acceso

Para poder usar una aplicación será necesario introducir o teclear, al menos, la contraseña que el usuario posea, sin perjuicio de la utilización de otros mecanismos adicionales que incrementen el nivel de seguridad de la aplicación.

Artículo 6. Control de acceso. Accesos especiales y vigencia de accesos

1. La aplicación no debe permitir la utilización de claves compartidas o multiusuarios, por tanto la clave debe ser un identificador único, personal e intransferible del usuario.

2. L'aplicació posseirà punts d'accés independents del repte de les funcionalitats de l'aplicació per a que els usuaris amb privilegis especials, aquells que permeten alterar certs controls de seguretat, puguen realitzar les seues funcions de seguretat.

3. L'aplicació avisarà, per a procedir a la seua eventual eliminació, d'aquells codis d'usuari que no hagen sigut utilitzats en el termini màxim de tres mesos.

4. Així mateix, en aquelles aplicacions en què l'usuari puga canviar lliurement la seua contrasenya, el sistema avisarà d'aquelles claus d'accés que es troben vençudes.

Article 7. Control d'accés. Contrasenyes

1. L'aplicació no ha de mostrar la contrasenya quan s'estiga teclejant

2. L'aplicació emmagatzemarà les contrasenyes mitjançant algoritmes de xifrat. Els arxius on es guarden les contrasenyes seran distints dels que contenen dades. L'aplicació no contindrà l'algoritme de desxifrat de les contrasenyes.

3. Les aplicacions que permeten a l'usuari escollir la seua pròpia contrasenya han de realitzar els controls següents:

a) Obligarà que les contrasenyes posseïsquen una longitud mínima de sis caràcters, així com la inclusió de l'algun tipus de caràcter distint de l'alfabètic.

b) Forçarà els usuaris a canviar les contrasenyes cada 3 mesos, com a màxim.

c) La contrasenya proporcionada inicialment a l'usuari es considerarà provisional i obligarà al seu canvi en la primera connexió a l'aplicació.

d) Han d'evitar la repetició de contrasenyes.

Article 8. Control d'accés: portes falses

Les aplicacions no hauran de posseir algoritmes o mecanismes que permeten la utilització de portes falses, com mitjans excepcionals d'accés al sistema d'informació.

Article 9. Control d'accés: accessos de terceres parts

1. Els sistemes, o servidors d'aplicació, hauran d'estar protegits mitjançant un sistema de tallafocs que restringisca els accessos als estrictament necessaris, en el cas de comunicacions amb terceres parts.

2. En cap dels casos, els sistemes tallafocs s'ubicaran en les mateixes màquines on residisquen les dades o les aplicacions.

Article 10. Control d'accés: inactivitat del sistema

1. En la mesura en què tecnològicament siga factible, les aplicacions, o els mitjans que les suporten, posseiran mecanismes que desconnecten l'accés de l'usuari a l'aplicació si el mateix no hi ha interactuat amb l'aplicació o amb els mitjans que la suporten, en el termini establit pel manual de seguretat de l'aplicació.

2. En aquells casos particulars en què aquesta mesura no s'implante directament sobre l'aplicació, sinó sobre altres mitjans auxiliars que suporten la seua execució (sistemes operatius, salvapantalles, etc.), aquest fet vindrà referit en el manual d'instal·lació de l'aplicació, com també en el manual de seguretat d'aquesta.

Article 11. Control d'accés: sistemes operatius

En aquells casos en què els sistemes operatius, sistemes de suport, o qualsevol altra classe d'eina, permeten accedir a la informació emmagatzemada per les aplicacions, sense necessitat de passar els mecanismes de seguretat d'aquestes, s'hauran d'implantar les mesures tècniques o d'organització necessàries per a restringir l'accés a la informació a les persones realment autoritzades.

Article 12. Integritat. Processos amb múltiples actualitzacions

Les aplicacions que executen transaccions o processos on es produïsquen múltiples actualitzacions de dades, les quals es troben relacionades entre si, hauran de posseir eines o mecanismes que asseguren la integritat d'aquestes dades, relacionades en el cas que es produïsca una fallada de procés i no es puga completar la transacció.

2. La aplicación poseerá puntos de acceso independientes del reto de las funcionalidades de la aplicación para que los usuarios con privilegios especiales, aquellos que permiten alterar ciertos controles de seguridad, puedan realizar sus funciones de seguridad.

3. La aplicación avisará, para proceder a su eventual eliminación, de aquellos códigos de usuario que no hayan sido utilizados en el plazo máximo de tres meses.

4. Asimismo, en aquellas aplicaciones en que el usuario pueda cambiar libremente su contraseña, el sistema avisará de aquellas claves de acceso que se encuentren vencidas.

Artículo 7. Control de acceso. Contraseñas

1. La aplicación no debe mostrar la contraseña cuando se esté tecleando

2. La aplicación almacenará las contraseñas mediante algoritmos de cifrado. Los archivos donde se guarden las contraseñas serán distintos de los que contienen datos. La aplicación no contendrá el algoritmo de descifrado de las contraseñas.

3. Las aplicaciones que permitan al usuario elegir su propia contraseña deben realizar los siguientes controles:

a) Obligará a que las contraseñas posean una longitud mínima de seis caracteres así como la inclusión del algún tipo de carácter distinto del alfabético.

b) Forzará a los usuarios a cambiar las contraseñas cada tres meses como máximo

c) La contraseña proporcionada inicialmente al usuario se considerará provisional y obligará a su cambio en la primera conexión a la aplicación

d) Deben evitar la repetición de contraseñas

Artículo 8. Control de acceso: Puertas falsas

Las aplicaciones no deberán poseer algoritmos o mecanismos que permitan la utilización de puertas falsas como medios excepcionales de acceso al sistema de información.

Artículo 9. Control de acceso: Accesos de terceras partes

1. Los sistemas o servidores de aplicación deberán estar protegidos mediante un sistema de cortafuegos que restrinja los accesos a los estrictamente necesarios en el caso de comunicaciones con terceras partes.

2. En ningún caso los sistemas cortafuegos se ubicarán en las mismas máquinas donde residan los datos o las aplicaciones.

Artículo 10. Control de acceso: Inactividad del sistema

1. En la medida en que tecnológicamente sea factible las aplicaciones, o los medios que las soporten, poseerán mecanismos que desconecten el acceso del usuario a la aplicación si el mismo no ha interactuado con la aplicación o con los medios que la soporten en el plazo establecido por el manual de seguridad de la aplicación.

2. En aquellos casos particulares en los que esta medida no se implante directamente sobre la aplicación sino sobre otros medios auxiliares que soportan su ejecución (sistemas operativos, salvapantallas, etc.), este hecho vendrá referido en el manual de instalación de la aplicación así como en el manual de seguridad de la misma.

Artículo 11. Control de acceso: Sistemas operativos

En aquellos casos en que los sistemas operativos, sistemas de soporte, o cualquier otra clase de herramienta, permitan acceder a la información almacenada por las aplicaciones sin necesidad de pasar los mecanismos de seguridad de éstas, entonces se deberán implantar las medidas técnicas o de organización necesarias para restringir el acceso a la información a las personas realmente autorizadas.

Artículo 12. Integridad. Procesos con múltiples actualizaciones

Las aplicaciones que ejecuten transacciones o procesos donde se produzcan múltiples actualizaciones de datos, los cuales se encuentren relacionados entre sí, deberán poseer herramientas o mecanismos que aseguren la integridad de estos datos relacionados en el caso de que se produzca un fallo de proceso y no se pueda completar la transacción.

Article 13. Integritat. Informacions confidencials

En aquells supòsits en què l'anàlisi de riscos determine que la informació qualificada com a confidencial no es troba suficientment protegida amb el control d'accessos, dita informació s'haurà de xifrar sobre el suport d'emmagatzemament.

Article 14. Integritat. Proteccions antivirus

1. Quan les aplicacions s'implanten sobre servidors d'aplicació que potencialment pogueren ser atacats per virus informàtics, dits servidors hauran de posseir proteccions antivirus residents en totes les unitats de procés que intervinguen en l'execució del sistema d'informació.

2. En aquells casos on els equips dels usuaris pogueren potencialment ser atacats per virus informàtics, aquests equips han de posseir proteccions antivirus.

3. El manual de seguretat de l'aplicació haurà de dedicar un capítol als procediments de protecció antivirus, tant d'operació com d'usuari.

Article 15. Disponibilitat

Els servidors d'aplicació han de complir les mesures següents:

1. Els equips que suporten determinats processos, la interrupció accidental dels quals puga provocar alteració o pèrdua de dades o documents administratius, han d'estar protegits contra fallades de subministrament elèctric mitjançant sistemes d'alimentació ininterrompuda.

2. Els equips que suporten processos especialment crítics han de ser equips d'alta disponibilitat, que posseïsquen mecanismes tolerants a les fallades.

3. Els equips han de mantenir-se d'acord amb les especificacions dels subministradors de servei.

4. Les àrees físiques on es troben situats els equips han de trobar-se convenientment, i han d'assegurar-se front a riscos derivats d'accessos no desitjats així com a amenaces d'entorn, tals com focs, fums, aigua, etc.

Article 16. Traçabilitat

Les aplicacions han d'estar dotades de pistes d'auditories, que hauran de registrar el codi d'usuari, data, hora i procés mitjançant el qual s'ha realitzat un alta, modificació o baixa de qualsevol informació que substancie l'exercici d'una potestat o d'aquella informació qualificada com a sensible.

Article 17. Comunicacions electròniques de dades

Quan es transmeten informacions o dades, l'aplicació o els mitjans i suports emprats per a la transmissió hauran de posseir, en el supòsit que les xarxes de transmissió no es consideren totalment segures, mecanismes que criptografien, en tot o en part, el contingut de la transmissió. Aquelles dades considerades confidencials se criptografiaran en la seua totalitat.

Article 18. Transmissió de contrasenyes

Quan es transmeten contrasenyes, o en general qualsevol informació que permeta garantir la integritat, autenticitat i confidencialitat de les transmissions, dits codis o informacions es transmetran criptografiats en la seua totalitat.

Article 19. Transmissió d'informacions sensibles

Quan les informacions sensibles han de ser transmeses caldrà criptografiar-les prèviament.

Article 20. Autentificació, integritat i no repudi en comunicacions

1. L'aplicació, o bé els mitjans o suports emprats en la transmissió, haurà de ser capaç de proveir de certificats d'autenticitat, emesos per l'autoritat autentificadora, per a totes aquelles comunicacions en què el receptor necessite garanties de la identitat de l'altra part i que la transmissió no ha sigut alterada.

Artículo 13. Integridad. Informaciones confidenciales

En aquellos supuestos en que el análisis de riesgos determine que la información calificada como confidencial no se encuentra suficientemente protegida con el control de accesos, dicha información se deberá cifrar sobre el soporte de almacenamiento.

Artículo 14. Integridad. Protecciones antivirus

1. Cuando las aplicaciones se implanten sobre servidores de aplicación que potencialmente pudieran ser atacados por virus informáticos, dichos servidores deberán poseer protecciones antivirus residentes en todas las unidades de proceso que intervengan en la ejecución del sistema de información.

2. En aquellos casos donde los equipos de los usuarios pudieran potencialmente ser atacados por virus informáticos, estos equipos deben poseer protecciones antivirus.

3. El manual de seguridad de la aplicación deberá dedicar un capítulo a los procedimientos de protección antivirus, tanto de operación como de usuario

Artículo 15. Disponibilidad

Los servidores de aplicación deben cumplir las siguientes medidas:

1. Los equipos que soporten determinados procesos, cuya interrupción accidental pueda provocar alteración o pérdida de datos o documentos administrativos, deben estar protegidos contra fallos de suministro eléctrico mediante sistemas de alimentación ininterrumpida.

2. Los equipos que soporten procesos especialmente críticos deben ser equipos de alta disponibilidad, que posean mecanismos tolerantes a fallos.

3. Los equipos deben mantenerse de acuerdo con las especificaciones de los suministradores de servicio.

4. Las áreas físicas donde se encuentren situados los equipos deben encontrarse convenientemente aseguradas frente a riesgos derivados de accesos indeseados así como amenazas de entorno, tales como fuegos, humos, agua, etc.

Artículo 16. Trazabilidad

Las aplicaciones deben estar dotadas de pistas de auditorías, que deberán registrar el código de usuario, fecha, hora y proceso mediante el que se ha realizado un alta, modificación o baja de cualquier información que sustancie el ejercicio de una potestad o de aquella información calificada como sensible.

Artículo 17. Comunicaciones electrónicas de datos

Cuando se transmitan informaciones o datos, la aplicación o los medios y soportes empleados para la transmisión deberán poseer, en el supuesto de que las redes de transmisión no se consideren totalmente seguras, mecanismos que criptografíen, en todo o en parte, el contenido de la transmisión. Aquellos datos considerados confidenciales se criptografiarán en su totalidad.

Artículo 18. Transmisión de contraseñas

Cuando se transmitan contraseñas, o en general cualquier información que permita garantizar la integridad, autenticidad y confidencialidad de las transmisiones, dichos códigos o informaciones se transmitirán criptografiados en su totalidad.

Artículo 19. Transmisión de informaciones sensibles

Cuando las informaciones sensibles deban ser transmitidas se deberán criptografiar previamente.

Artículo 20. Autenticación, integridad y no repudio en comunicaciones

1. La aplicación, o bien los medios o soportes empleados en la transmisión, deberá ser capaz de proveer de certificados de autenticidad, emitidos por la autoridad autentificadora, para todas aquellas comunicaciones en que el receptor necesite garantías de la identidad de la otra parte y de que la transmisión no ha sido alterada.

2. Per a aquelles aplicacions que requerisquen la garantia addicional del no repudi, l'aplicació, o bé els mitjans o suports emprats en la transmissió, hauran d'incorporar mecanismes que asseguren la irrenunciabilitat de la participació del transmissor i del receptor, quan es produïsquen comunicacions.

Article 21. Tercera part de confiança en les comunicacions

Les aplicacions, o bé els mitjans o suports emprats en la transmissió, gestionaran l'assignació de claus públiques, claus privades i els serveis de certificat a través dels mitjans i suports disposats per l'autoritat autentificadora, per a aquests fins.

CAPÍTOL II
Conservació de la informació

Article 22. Conservació de la informació de gestió

1. Es considera informació de gestió aquella que no ha sigut traspassada a altres arxius, centrals o històrics, en funció de la normativa de gestió documental aplicable.

2. Els servidors d'aplicació hauran de comptar amb un procés de salvament periòdic de les dades de les aplicacions. Aquests processos garantiran que el període màxim transcorregut, entre que una dada és canviada i salvada, no depasse els set dies.

3. Així mateix, hauran de comptar amb un mecanisme de reincorporació d'informació prèviament salvada, a executar en cas que es produïra una deterioració en el suport físic d'emmagatzemament de la informació.

4. L'aplicació haurà de posseir un procediment escrit en què es dictaran les instruccions necessàries per al salvament i la recuperació de la informació, així com el període de salvament.

5. En relació a la funcionalitat de l'aplicació, els informes preceptius d'aquesta, segons redacció de l'article 22.4 a) del Decret 96/1998, de 6 de juliol, hauran de definir el moment o termini en què, en absència d'impugnacions, la informació manca de vigència administrativa, segons definició de l'article 3 del Decret 57/1984, de 21 de maig.

6. Amb una periodicitat mínima anual, s'efectuarà un procediment de recuperació d'informació salvada, a fi de verificar que el procés de salvament s'està efectuant correctament.

Article 23. Compactació de la informació de gestió

1. Quan no es trobe garantit que el servidor d'aplicació puga mantenir les dades de gestió activament, llavors l'aplicació posseirà un procés de compactació que haurà de permetre eliminar del suport d'emmagatzemament, i amb una periodicitat donada, aquelles dades que no siguen utilitzades per a l'exercici de potestats. Per tant, el procés de compactació extraurà només aquella informació que substancie el contingut d'actes administratius.

2. En el cas que les dades compactades siguen, alhora, salvades en en un altre suport d'emmagatzemament, i, tot seguit, siguen eliminades del suport de gestió, haurà d'existir un altre procés que permeta reincorporar les dades compactades, de forma que siguen llegibles per l'aplicació.

3. Les dades compactades han de mantenir-se accessibles als usuaris de l'aplicació, fins que dita informació adquirisca el caràcter d'històrica en funció de la normativa aplicable.

4. La informació que pertanya a expedients actius, no arxivats, no estarà subjecta al procés de compactació.

5. L'aplicació haurà de comptar amb algun mecanisme que permeta marcar els expedients que es troben impugnats. Aquests expedients no seran sotmesos a compactació

Article 24. Canvis de versions, sistemes operatius o noves aplicacions

1. Quan l'aplicació siga substituïda per una nova aplicació, aquesta última haurà de posseir els mecanismes necessaris per a incorporar tota la informació existent fins aqueix moment, de gestió

2. Para aquellas aplicaciones que requieran la garantía adicional del no repudio, la aplicación, o bien los medios o soportes empleados en la transmisión, deberán incorporar mecanismos que aseguren la irrenunciabilidad de la participación del transmisor y del receptor cuando se produzcan comunicaciones.

Artículo 21. Tercera parte de confianza en las comunicaciones

Las aplicaciones, o bien los medios o soportes empleados en la transmisión, gestionarán la asignación de claves públicas, claves privadas y los servicios de certificación a través de los medios y soportes dispuestos por la Autoridad Autentificadora para estos fines.

CAPÍTULO II
Conservación de la información

Artículo 22. Conservación de la información de gestión

1. Se considera información de gestión aquella que no ha sido traspasada a otros archivos, centrales o históricos, en función de la normativa de gestión documental aplicable.

2. Los servidores de aplicación deberán contar con un proceso de salvado periódico de los datos de las aplicaciones. Estos procesos garantizarán que el período máximo transcurrido entre que un dato es cambiado y el dato es salvado no podrá exceder de siete días.

3. Asimismo, deberán contar con un mecanismo de reincorporación de información previamente salvada, a ejecutar en caso de que se produjera un deterioro en el soporte físico de almacenamiento de la información.

4. La aplicación deberá poseer un procedimiento escrito en el cual se dictarán las instrucciones necesarias para el salvado y la recuperación de la información, así como el período de salvado.

5. En relación a la funcionalidad de la aplicación, los informes preceptivos de la misma, según redacción del artículo 22.4 a) del Decreto 96/1998, de 6 de julio, deberán definir el momento o plazo en que, en ausencia de impugnaciones, la información carece de vigencia administrativa, según definición del artículo 3 del Decreto 57/1984, de 21 de mayo.

6. Con una periodicidad mínima anual se efectuará un procedimiento de recuperación de información salvada con la finalidad de verificar que el proceso de salvado se está efectuando correctamente.

Artículo 23. Compactación de la información de gestión

1. Cuando no se encuentre garantizado que el servidor de aplicación pueda mantener los datos de gestión activamente entonces la aplicación poseerá un proceso de compactación que deberá permitir eliminar del soporte de almacenamiento, con una periodicidad dada, aquellos datos que no sean utilizados para el ejercicio de potestades. Por tanto, el proceso de compactación extraerá solamente aquella información que sustancie el contenido de actos administrativos.

2. En el caso de que los datos compactados sean a su vez salvados a otro soporte de almacenamiento, y a continuación sean eliminados del soporte de gestión, deberá existir otro proceso que permita reincorporar los datos compactados de forma que sean legibles por la aplicación.

3. Los datos compactados deben mantenerse accesibles a los usuarios de la aplicación hasta que dicha información adquiera el carácter de histórica en función de la normativa aplicable.

4. La información que pertenezca a expedientes activos, no archivados, no estará sujeta al proceso de compactación.

5. La aplicación deberá contar con algún mecanismo que permita marcar los expedientes que se encuentren impugnados. Estos expedientes no serán sometidos a compactación

Articulo 24. Cambios de versiones, sistemas operativos o nuevas aplicaciones

1. Cuando la aplicación sea sustituida por una nueva aplicación, esta última deberá poseer los mecanismos necesarios para incorporar toda la información existente hasta ese momento, de gestión y

i compactada, al seu nou format. Només es permetrà la no incorporació, o la incorporació parcial, quan es trobe garantit el manteniment dels mitjans i suports que permeten accedir a la informació no incorporada.

2. Si una aplicació deixa d'utilitzar-se, i el seu funcionalitat no és substituïda per una nova aplicació, s'estarà als següents casos:

Si el manteniment dels suports i mitjans que executen dita aplicació es troba garantit en el termini en què les dades han de ser conservades, tant l'aplicació com els suports hauran de ser mantinguts, com també la documentació necessària per a l'explotació del sistema.

b) Si el manteniment no es troba garantit, aleshores les dades bàsiques de l'aplicació de caràcter no històric hauran de ser traspassades a un nou format, la durabilitat del qual es trobe garantida

Article 25. Conservació de dades personals

1. Les dades personals especialment sensibles, segons es defineixen en l'article 7 de la Llei Orgànica 5/1992, de 29 d'octubre, que reflectisquen situacions transitòries, no seran incloses en el conjunt d'informació que sofrisca el procés de compactació.

2. Les dades personals referides en el paràgraf anterior hauran de ser eliminades completament del suport d'emmagatzemament, en el moment en què dita situació haja finalitzat.

CAPÍTOL III
Tractament dels documents electrònics

Article 26. Documents electrònics i aplicacions

1. L'aplicació ha de recollir entre les seues pròpies funcionalitats, si fa el cas, el tractament dels documents electrònics pertanyents als procediments administratius gestionats.

2. S'haurà de publicar els distints tipus de documents electrònics que són gestionats per l'aplicació, relacionant-los amb els seus respectius procediments, així com el mode d'accés als mateixos, si fa el cas.

3. Les especificacions de l'aplicació hauran de detallar l'arquitectura adoptada per al tractament dels distints tipus de documents gestionats, incloent les possibilitats de consulta i transmissió.

Article 27. Accessibilitat dels documents electrònics

Les aplicacions que gestionen documents electrònics hauran de posseir connectivitat a la Xarxa Corporativa de la Generalitat Valenciana, de manera que qualsevol persona, amb els permisos adequats, puga consultar aquests documents.

Article 28. Característiques dels documents electrònics

Un document electrònic ha de reunir les característiques següents:

a) Ha de trobar-se en la ubicació electrònica assignada al document

b) Ha de contenir o posseir un codi de validació, segons s'especifica en l'article 29.

c) El seu format ha de pertànyer a algun dels establits en els estàndards informàtics de la Generalitat Valenciana, aprovats pel Comité Tècnic per al Desplegament dels Sistemes d'Informació

Article 29. Codis de validació dels documents electrònics

1. Els codis de validació dels documents electrònics han d'haver sigut generats mitjançant tècniques de xifrat, a partir de les següents dades, com a mínim:

a) Contingut del document electrònic.

b) Data i hora de generació del document electrònic.

2. Els codis de validació es podran guardar físicament de les maneres següents:

a) Com a part del contingut del document, addicionalment a la informació que substància l'acte administratiu.

compactada, a su nuevo formato. Solamente se permitirá la no incorporación o la incorporación parcial cuando se encuentre garantizado el mantenimiento de los medios y soportes que permitan acceder a la información no incorporada.

2. Si una aplicación deja de utilizarse y su funcionalidad no es sustituida por una nueva aplicación se estará en los siguientes casos:

a) Si el mantenimiento de los soportes y medios que ejecutan dicha aplicación se encuentra garantizado en el plazo en que los datos deben ser conservados, tanto la aplicación como los soportes deberán ser mantenidos, así como la documentación necesaria para la explotación del sistema

b) Si el mantenimiento no se encuentra garantizado, entonces los datos básicos de la aplicación de carácter no histórico deberán ser traspasados a un nuevo formato cuya durabilidad se encuentre garantizada

Artículo 25. Conservación de datos personales

1. Los datos personales especialmente sensibles, según se definen en el artículo 7 de la Ley Orgánica 5/1992, de 29 de octubre, que reflejen situaciones transitorias no serán incluidos en el conjunto de información que sufra el proceso de compactación.

2. Los datos personales referidos en el párrafo anterior deberán ser eliminados completamente del soporte de almacenamiento en el momento en que dicha situación haya finalizado.

CAPÍTULO III
Tratamiento de los documentos electrónicos

Artículo 26. Documentos electrónicos y aplicaciones

1. La aplicación debe recoger entre sus propias funcionalidades, en su caso, el tratamiento de los documentos electrónicos pertenecientes a los procedimientos administrativos gestionados.

2. Se deberá publicar los distintos tipos de documentos electrónicos que son gestionados por la aplicación, relacionándolos con sus respectivos procedimientos, así como el modo de acceso a los mismos, en su caso.

3. Las especificaciones de la aplicación deberán detallar la arquitectura adoptada para el tratamiento de los distintos tipos de documentos gestionados, incluyendo las posibilidades de consulta y transmisión.

Artículo 27. Accesibilidad de los documentos electrónicos

Las aplicaciones que gestionen documentos electrónicos deberán poseer conectividad a la Red Corporativa a la Generalitat Valenciana, de modo que cualquier persona con los permisos adecuados pueda consultar estos documentos.

Artículo 28. Características de los documentos electrónicos

Un documento electrónico debe reunir las siguientes características:

a) Debe encontrarse en la ubicación electrónica asignada al documento

b) Debe contener o poseer un código de validación según se especifica en el artículo 29

c) Su formato debe pertenecer a alguno de los establecidos en los Estándares Informáticos de la Generalitat Valenciana, aprobados por el Comité Técnico para el Desarrollo de los Sistemas de Información

Artículo 29. Códigos de validación de los documentos electrónicos

1. Los códigos de validación de los documentos electrónicos deben haber sido generados mediante técnicas de cifrado a partir de los siguientes datos, como mínimo:

a) Contenido del documento electrónico

b) Fecha y hora de generación del documento electrónico

2. Los códigos de validación se podrán guardar físicamente de las siguientes formas:

a) Como parte del contenido del documento, adicionalmente a la información que sustancia el acto administrativo

b) Com una informació annexa, el suport de la qual posseirà una relació biunívoca amb el suport que conté al document.

c) En un camp de la base de dades controlades per l'aplicació que gestiona els documents electrònics.

Article 30. Alteració i supressió de documents electrònics

1. Els documents electrònics no es podran alterar en cap cas.

2. Aquests mateixos documents electrònics només es podran suprimir, una vegada finalitzat el procediment i mitjançant els processos de conservació d'informació establits, sempre que es respecte allò establit en l'article 31.

3. Igualment, ni els suports ni els camps de base de dades on s'emmagatzemen els codis de validació, segons s'estableix en l'article 29, podran ser objecte d'alteració. Només podran ser eliminats, en aquests mateixos processos de conservació, quan es mantinga la coherència de la informació entre els documents i els seus codis de validació.

Article 31. Requeriments de les aplicacions

Les aplicacions que gestionen documents electrònics han de posseir enllaços amb aquests, de forma que es complisca el següent:

a) L'enllaç s'ha d'establir en el moment i en el tràmit en què el document és generat

b) Si un document és substituït per un altre, es mantindrà l'enllaç a ambdós documents, indicant quin és el document activament i actualment vàlid. Aquest punt no s'aplicarà quan aquesta substitució es produïsca com a rectificació d'errors materials, de fet o aritmètics, en concordança amb allò que s'ha establit en l'article 105 de la Llei 30/1992, de 26 de novembre.

TÍTOL III
Mesures d'organització aplicables a la seguretat i conservació de les aplicacions

CAPÍTOL I
El sistema de seguretat

Article 32. Del responsable de l'aplicació

El responsable de l'aplicació és una persona, pertanyent a la unitat, que utilitzarà l'aplicació per a l'exercici de les seues potestats, designat per aquesta mateixa unitat abans de l'inici de l'explotació de l'aplicació, i que posseeix les següents funcions:

1. Designar i autoritzar els usuaris que han d'utilitzar l'aplicació.

2. Assignar els accessos a què es permet a cada usuari, motivant aquests.

3. Autoritzar aquelles cessions de dades no previstes en l'aplicació, en la forma legalment prevista.

4. Definir els terminis en què la informació deixa de tindre vigència administrativa, podent ampliar, de forma motivada, el moment o termini en què la informació corresponent a determinats expedients deixa de tindre vigència administrativa, degut a l'existència d'impugnacions o al requeriment de l'autoritat judicial o d'algun dels òrgans de control de l'administració.

5. Autoritzar, per escrit, l'inici de l'explotació de l'aplicació.

Article 33. Del responsable de seguretat

1. El responsable de seguretat és aquella persona la missió de la qual consisteix a garantir la seguretat d'explotació d'una aplicació.

2. El responsable de seguretat serà designat per l'autoritat autentificadora, a proposta de la Unitat Informàtica corresponent, d'acord amb l'article 20.a del Decret 96/1998, de 6 de juliol.

3. El responsable de seguretat ha d'haver intervingut en el procediment d'aprovació de l'aplicació.

4. El responsable de seguretat ha de ser designat abans del moment en què comence l'explotació de l'aplicació.

b) Como una información anexa, cuyo soporte poseerá una relación biunívoca con el soporte que contiene al documento.

c) En un campo de la base de datos controlada por la aplicación que gestiona los documentos electrónicos

Artículo 30. Alteración y supresión de documentos electrónicos

1. Los documentos electrónicos no se podrán alterar en ningún caso.

2. Estos mismos documentos electrónicos solamente se podrán suprimir, una vez finalizado el procedimiento y mediante los procesos de conservación de información establecidos, siempre que se respete lo establecido en el artículo 31.

3. Del mismo modo, ni los soportes ni los campos de base de datos donde se almacenen los códigos de validación, según se establece en el artículo 29, podrán ser objeto de alteración. Solamente podrán ser eliminados en estos mismos procesos de conservación de forma que se mantenga la coherencia de la información entre los documentos y sus códigos de validación.

Artículo 31. Requerimientos de las aplicaciones

Las aplicaciones que gestionen documentos electrónicos deben poseer enlaces a los mismos de forma que se cumpla lo siguiente:

a) El enlace se debe establecer en el momento y en el trámite en el que el documento es generado

b) Si un documento es sustituido por otro, se mantendrá el enlace a ambos documentos, indicando cual es el documento activo y actualmente válido. Este punto no aplicará cuando esta sustitución se produzca como rectificación de errores materiales, de hecho o aritméticos, en concordancia con lo establecido en el artículo 105 de la ley 30/1992, de 26 de noviembre.

TÍTULO III
Medidas de organización aplicables a la seguridad y conservación de las aplicaciones

CAPÍTULO I
El sistema de seguridad

Artículo 32. Del responsable de la aplicación

El responsable de la aplicación es una persona perteneciente a la unidad que utilizará la aplicación para el ejercicio de sus potestades, designado por esta misma unidad antes del inicio de la explotación de la aplicación, y que posee las siguientes funciones:

1. Designar y autorizar a los usuarios que deben utilizar la aplicación

2. Asignar los accesos a que se permite a cada usuario, motivando los mismos

3. Autorizar aquellas cesiones de datos no previstas en la aplicación en la forma legalmente prevista

4. Definir los plazos en los que la información deja de tener vigencia administrativa, pudiendo ampliar, de forma motivada, el momento o plazo en que la información correspondiente a determinados expedientes deja de tener vigencia administrativa, debido a la existencia de impugnaciones o al requerimiento de la autoridad judicial o de alguno de los órganos de control de la administración.

5. Autorizar, por escrito, el inicio de la explotación de la aplicación

Artículo 33. Del responsable de seguridad

1. El responsable de seguridad es aquella persona cuya misión consiste en garantizar la seguridad de explotación de una aplicación.

2. El responsable de seguridad será designado por la autoridad autentificadora, a propuesta de la Unidad Informática correspondiente, de acuerdo con el artículo 20.a del Decreto 96/1998, de 6 de julio.

3. El responsable de seguridad debe haber intervenido en el procedimiento de aprobación de la aplicación.

4. El responsable de seguridad debe ser designado antes del momento en que comience la explotación de la aplicación.

5. El responsable de seguretat ha de rebre la formació adequada en la gestió de seguretat d'aqueixa aplicació concreta.

6. L'aplicació no es posarà en marxa sense l'autorització expressa, i per escrit, del responsable de seguretat.

Article 34. Dels usuaris

Els usuaris de les aplicacions, en l'ús de les mateixes per a l'exercici de les seues funcions, tenen les obligacions mínimes següents:

a) Responsabilitat en el manteniment de les claus d'accés. L'usuari té el deure de guardar secret en relació amb aquestes.

b) Notificar al responsable de seguretat quan el secret de la seua contrasenya s'haja vist compromesa.

c) Obligació de tancar l'aplicació quan s'abandone el lloc de treball.

d) Obligació de comunicació de les incidències de seguretat al responsable de seguretat

Article 35. Verificacions de seguretat

1. El responsable de seguretat ha de verificar l'existència d'una sèrie de procediments de seguretat i conservació, abans d'autoritzar l'arrancada d'una aplicació.

2. Aquests procediments, que han de figurar per escrit, són els següents:

a) Mecanismes de seguretat d'usuari.

b) Procediments de salvament i de recuperació.

c) Procediments de contingència.

d) Procediments de compactació, si fa el cas.

3. En aquests procediments cal especificar, com a mínim, el següent:

a) Relació de tasques a executar i dels processos implicats.

b) Resultat de cada tasca i procés.

c) Responsable de cadascuna de les tasques.

d) Periodicitat.

e) Documentació a complimentar en cada operació.

Article 36. Gestió del registre de codis d'usuari

1. En compliment d'allò establit en l'article 21 del Decret 96/1998, de 6 de juliol, el responsable de seguretat ha de mantenir un registre dels codis d'usuari de l'aplicació.

2. No es podrà donar d'alta un usuari, o modificar els drets d'accés d'aquest a l'aplicació, si prèviament no ha sigut donat d'alta en el registre.

3. El responsable de seguretat haurà de mantenir actualitzat aquest registre, mantenint la història del mateix a través de les següents actuacions:

a) A partir de les notificacions del responsable de l'aplicació.

b) A partir dels avisos de l'aplicació de codis d'accés vençuts.

c) Validació periòdica, amb el concurs del responsable d'aplicació, dels usuaris de l'aplicació, definits així com els seus nivells d'accés.

4. Així mateix, realitzarà les actuacions corresponents en l'aplicació, a fi d'actualitzar correctament els drets d'accés de cada usuari.

5. Amb una periodicitat trimestral, el responsable de seguretat haurà de sotmetre, a revisió exhaustiva, tots els permisos amb privilegis existents en l'aplicació.

Article 37. Drets d'accés d'usuaris

D'acord amb les especificacions de disseny, i amb les instruccions de la unitat competent, el responsable de seguretat ha de crear i mantenir actualitzada una normativa escrita que definisca els drets d'accés a l'aplicació de cada usuari o grup d'usuaris.

Article 38. Relació d'incidències

1. El responsable de seguretat haurà de mantenir una relació d'incidències on es recullen totes aquelles situacions i esdeveniments que hagen suposat una minva de la seguretat de l'aplicació

5. El responsable de seguridad debe recibir la formación adecuada en la gestión de seguridad de esa aplicación concreta.

6. La aplicación no se podrá en marcha sin la autorización expresa, y por escrito, del responsable de seguridad.

Artículo 34. De los usuarios

Los usuarios de las aplicaciones, en el uso de las mismas para el ejercicio de sus funciones, tienen las siguientes obligaciones mínimas:

a) Responsabilidad en el mantenimiento de las claves de acceso. El usuario tiene el deber de secreto con relación a las mismas

b) Notificar al responsable de seguridad cuando el secreto de su contraseña se haya visto comprometido

c) Obligación de cerrar la aplicación cuando se abandone el puesto de trabajo

d) Obligación de comunicación de las incidencias de seguridad al responsable de seguridad

Artículo 35. Verificaciones de seguridad

1. El responsable de seguridad debe verificar la existencia de una serie de procedimientos de seguridad y conservación antes de autorizar el arranque de una aplicación.

2. Estos procedimientos, que deben figurar por escrito, son los siguientes:

a) Mecanismos de seguridad de usuario

b) Procedimientos de salvado y recuperación

c) Procedimientos de contingencia

d) Procedimientos de compactación, en su caso

3. En estos procedimientos se debe especificar, como mínimo, lo siguiente:

a) Relación de tareas a ejecutar y procesos implicados

b) Resultado de cada tarea y proceso

c) Responsable de cada una de las tareas

d) Periodicidad

e) Documentación a cumplimentar en cada operación

Artículo 36. Gestión del registro de códigos de usuario

1. En cumplimiento de lo establecido en el artículo 21 del Decreto 96/1998, de 6 de julio, el responsable de seguridad debe mantener un registro de los códigos de usuario de la aplicación.

2. No se podrá dar de alta un usuario o modificar los derechos de acceso del mismo a la aplicación si previamente no ha sido dado de alta en este registro.

3. El responsable de seguridad deberá mantener actualizado este registro, manteniendo la historia del mismo, a través de las siguientes actuaciones:

a) A partir de las notificaciones del responsable de la aplicación

b) A partir de los avisos de la aplicación de códigos de acceso vencidos

c) Validación periódica, con el concurso del responsable de aplicación, de los usuarios de la aplicación definidos así como sus niveles de acceso

4. Asimismo, realizará las actuaciones correspondientes en la aplicación con el fin de actualizar correctamente los derechos de acceso de cada usuario.

5. Con una periodicidad trimestral, el responsable de seguridad deberá someter a revisión exhaustiva todos los permisos con privilegios existentes en la aplicación.

Artículo 37. Derechos de acceso de usuarios

De acuerdo con las especificaciones de diseño y con las instrucciones de la unidad competente, el responsable de seguridad debe crear y mantener actualizada una normativa escrita que defina los derechos de acceso a la aplicación de cada usuario o grupo de usuarios.

Artículo 38. Relación de incidencias

1. El responsable de seguridad deberá mantener una relación de incidencias donde se recojan todas aquellas situaciones y acontecimientos que hayan supuesto una merma de la seguridad de la apli-

en un moment donat. En aquesta relació han de figurar les dades següents:

a) Codi(s) d'usuari(s) involucrats en la incidència.

b) Procés i funció involucrats.

c) Dades involucrades.

d) Descripció de la incidència.

e) Actuacions realitzades per a evitar la seua repetició.

2. El responsable de seguretat haurà de mantenir actualitzada aquesta relació a partir de les incidències que detecte o bé per les incidències comunicades, bé per les unitats competents o els seus usuaris, bé pel responsable de la unitat d'informàtica a què es troben adscrits els servidors d'aplicació.

3. El responsable de seguretat notificarà les incidències de seguretat a l'autoritat autentificadora.

Article 39. Control d'incidències

1. El responsable de seguretat efectuarà una anàlisi d'incidències de seguretat, amb una periodicitat mensual. Els resultats d'aquesta anàlisi, així com les accions que es decidisquen iniciar com a conseqüència de la mateixa, seran notificats, per escrit a l'autoritat autentificadora. A més, es remetran al responsable d'aplicació aquelles incidències relacionades amb el seu àmbit d'actuació.

2. L'autoritat autentificadora efectuarà una anàlisi de totes les incidències ocorregudes en el seu àmbit d'actuació, amb una periodicitat trimestral.

3. Com a conseqüència d'aquesta anàlisi, i quan s'estime oportú, l'autoritat autentificadora emetrà circulars dirigides a tots els responsables de seguretat, on es proporcionaran instruccions conduents a elevar el nivell de seguretat de les aplicacions.

CAPÍTOL II
Procediments de seguretat

Article 40. Alta, modificació i baixa d'usuaris

1. El responsable de l'aplicació comunicarà al responsable de seguretat les altes, modificacions i baixes d'usuaris, i li proporcionarà la informació necessària per a complimentar el registre d'usuaris.

2. Cada nou usuari de l'aplicació ha de firmar un document, denominat credencial de seguretat, que formalitze el seu accés a l'aplicació, i mitjançant el qual reconega la comprensió i acceptació de les condicions d'accés. En aquest document s'han d'explicitar els següents punts

2.1 A nivell general de l'aplicació

a) Totes les obligacions que es relacionen en l'article 34.

b) Normes particulars de seguretat de l'aplicació.

2.2 A nivell particular de l'usuari, o bé per tipus d'usuari:

a) Drets d'accés, açò és, funcionalitats i dades a què es troba autoritzat.

b) Drets d'accés amb privilegis, si fa el cas.

3. En el moment en què l'usuari firme la credencial, se li entregaran les seus claus d'accés. Una còpia del document li serà entregada a l'usuari.

4. Qualsevol canvi en les autoritzacions de seguretat comportarà l'emissió i firma d'una nova credencial.

Article 41. Formació d'usuaris

1. La formació en qüestions de seguretat, amb especial menció a la formació en mecanismes antivirus, ha de ser proporcionada com una part integrant de la formació en l'aplicació

2. El responsable de seguretat comprovarà, mitjançant el mètode que estime més adient, que els usuaris que reben la credencial coneixen les mesures de seguretat de l'aplicació

Article 42. Protecció antivirus

1. Sense perjudici que les aplicacions posseïsquen mecanismes antivirus, els usuaris que posseïsquen estacions de treball tipus PC hauran de comprovar que el seu equip posseeix instal·lat un sistema antivirus i que funciona correctament. El responsable de seguretat prestarà suport als usuaris per a realitzar aquesta comprovació.

cación en un momento dado. En esta relación se deben llevar los siguientes datos:

a) Código(s) de usuario(s) involucrados en la incidencia

b) Proceso y función involucrados

c) Datos involucrados

d) Descripción de la incidencia

e) Actuaciones realizadas para evitar su repetición

2. El responsable de seguridad deberá mantener actualizada esta relación a partir de las incidencias que detecte o bien por las incidencias comunicadas, bien por las unidades competentes o sus usuarios, bien por el responsable de la unidad de informática a la que se encuentren adscritos los servidores de aplicación.

3. El responsable de seguridad notificará las incidencias de seguridad a la autoridad autentificadora.

Artículo 39. Control de incidencias

1. El responsable de seguridad efectuará un análisis de incidencias de seguridad con una periodicidad mensual. Los resultados de este análisis, así como las acciones que se decidan iniciar como consecuencia del mismo, serán notificados, por escrito, a la autoridad autentificadora. Asimismo, se remitirán al responsable de aplicación aquellas incidencias relacionadas con su ámbito de actuación.

2. La autoridad autentificadora efectuará un análisis de todas las incidencias ocurridas en su ámbito de actuación con una periodicidad trimestral.

3. Como consecuencia de este análisis, y cuando se estime oportuno, la autoridad autentificadora emitirá circulares dirigidas a todos los responsables de seguridad donde se proporcionarán instrucciones conducentes a elevar el nivel de seguridad de las aplicaciones.

CAPÍTULO II
Procedimientos de seguridad

Artículo 40. Alta, modificación y baja de usuarios

1. El responsable de la aplicación comunicará al responsable de seguridad las altas, modificaciones y bajas de usuarios, proporcionándole la información necesaria para cumplimentar el registro de usuarios.

2. Cada nuevo usuario de la aplicación debe firmar un documento, denominado credencial de seguridad, que formalice su acceso a la aplicación y mediante el cual reconozca la comprensión y aceptación de las condiciones de acceso. En este documento se deben explicitar los siguientes puntos:

2.1 A nivel general de la aplicación:

a) Todas las obligaciones que se relacionan en el artículo 34

b) Normas particulares de seguridad de la aplicación

2.2 A nivel particular del usuario, o bien por tipos de usuario:

a) Derechos de acceso, esto es, funcionalidades y datos a los que se encuentra autorizado

b) Derechos de acceso con privilegios, en su caso

3. En el momento en que el usuario firme la credencial se le entregarán sus claves de acceso. Una copia del documento le será entregada al usuario.

4. Cualquier cambio en las autorizaciones de seguridad conllevará la emisión y firma de una nueva credencial

Artículo 41. Formación de usuarios

1. La formación en cuestiones de seguridad, con especial mención a la formación en mecanismos antivirus, debe ser proporcionada como una parte integrante de la formación en la aplicación

2. El responsable de seguridad comprobará, mediante el método que estime mas oportuno, que los usuarios que reciben la credencial conocen las medidas de seguridad de la aplicación

Artículo 42. Protección antivirus

1. Sin perjuicio de que las aplicaciones posean mecanismos antivirus, los usuarios que posean estaciones de trabajo tipo PC deberán comprobar que su equipo posee instalado un sistema antivirus y que funciona correctamente. El responsable de seguridad prestará soporte a los usuarios para realizar esta comprobación.

2. D'altra banda, el responsable de seguretat verificarà que les versions dels productes antivirus es troben correctament actualitzades. Es considerarà que succeeix una incidència quan el programa antivirus posseïsca una antiguitat superior a 6 mesos.

Article 43. Operació de les aplicacions

1. El responsable de seguretat verificarà que totes les tasques d'operació de l'aplicació es realitzen en temps i forma. S'entén per tasques d'operació les següents:

a) Salvament periòdic de dades.

b) Compactació de dades, si fa el cas.

2. En cas d'incompliment d'alguna d'aquestes, haurà de considerar aquest fet com una incidència, i com tal registrar-la.

3. Una còpia d'aquesta incidència, addicionalment al preceptiu enviament a l'autoritat autentificadora, serà enviada al responsable de la unitat d'informàtica en què es troben adscrits els servidors d'aplicació.

Article 44. Manteniment d'aplicacions

1. El responsable de seguretat haurà d'autoritzar prèviament la substitució de programes o elements de l'aplicació, quan aquests impliquen alteració de la funcionalitat de l'aplicació, en els termes establits en l'article 22.7 del Decret 96/1998.

2. Amb caràcter previ al canvi, el responsable de seguretat haurà d'aprovar els informes elaborats pel responsable del canvi, on s'especificarà i acreditarà, si més no, el següent:

a) Motiu del canvi.

b) Realització de proves que confirmen el bon funcionament dels programes o elements substituents.

c) Permanència de les mesures de seguretat que l'aplicació posseïsca.

d) Responsable/s del canvi.

3. El responsable de seguretat haurà de portar una relació de totes les substitucions de programes o elements de l'aplicació, registrant el moment en què aquests comencen a ser operatius.

Article 45. Procediment de contingència

1. Cada usuari ha de disposar d'una còpia del procediment de contingència, en aquells aspectes que l'afecten, en un lloc accessible. Així mateix, ha d'haver sigut instruït sobre les actuacions que ha d'executar en cada situació prevista.

2. Les situacions en què es produïsca una contingència han de ser registrades com una incidència.

3. Quan el responsable de seguretat ho estime oportú, podrà realitzar simulacres de situacions de contingència, a fi de verificar l'execució de les respostes adequades en cada cas.

4. Els resultats no previstos d'aquest simulacre han de registrar-se com a incidències.

Article 46. Elements de seguretat

1. Les ubicacions físiques on es troben els servidors d'aplicacions hauran de trobar-se en àrees tancades o àrees de seguretat.

2. La porta d'accés a aquesta àrea haurà de trobar-se permanentment tancada, i amb mecanismes per al control d'accessos a aquesta.

3. Aquests dispositius poden ser substituïts, alternativament, per un sistema d'accés mitjançant codis personals.

4. Els materials perillosos i/o combustibles han d'emmagatzemar-se en l'exterior de l'àrea i a una distància de seguretat de la sala d'ordinadors.

5. Els dispositius de salvament de dades (cintes, cassettes, etc.) s'emmagatzemaran en armaris ignífugs, preferentment en altres locals diferents a les àrees de seguretat. Aquests armaris estaran tancats de forma segura.

6. Ha d'instal·lar-se en l'àrea un adequat equipament de seguretat, com ara sistemes d'extinció, detectors de fums, etc.

7. El personal extern, que haja d'efectuar treballs en l'interior de l'àrea de seguretat, ha de trobar-se degudament autoritzat i identificat. El responsable de l'àrea estendrà una acreditació a favor d'aquest personal.

2. Por otro lado, el responsable de seguridad verificará que las versiones de los productos antivirus se encuentren correctamente actualizadas. Se considerará que sucede una incidencia cuando el programa antivirus posea una antigüedad superior a 6 meses.

Artículo 43. Operación de las aplicaciones

1. El responsable de seguridad verificará que todas las tareas de operación de la aplicación se realicen en tiempo y forma. Se entiende por tareas de operación las siguientes:

a) Salvado periódico de datos

b) Compactación de datos, en su caso

2. En caso de incumplimiento de alguna de las mismas, deberá considerar este hecho como una incidencia, y como tal registrarse.

3. Una copia de esta incidencia, adicionalmente al preceptivo envío a la autoridad autentificadora, será enviada al responsable de la unidad de informática a la que se encuentren adscritos los servidores de aplicación.

Artículo 44. Mantenimiento de aplicaciones

1. El responsable de seguridad deberá autorizar previamente la sustitución de programas o elementos de la aplicación, cuando éstos impliquen alteración de la funcionalidad de la aplicación, en los términos establecidos en el artículo 22.7 del Decreto 96/1998.

2. Con carácter previo al cambio, el responsable de seguridad deberá aprobar los informes elaborados por el responsable del cambio donde se especificará y acreditará, al menos, lo siguiente:

a) Motivo del cambio

b) Realización de pruebas que confirmen el buen funcionamiento de los programas o elementos sustituyentes

c) Permanencia de las medidas de seguridad que la aplicación posea

d) Responsable/s del cambio

3. El responsable de seguridad deberá llevar una relación de todas las sustituciones de programas o elementos de la aplicación, registrando el momento en que estos comienzan a ser operativos.

Artículo 45. Procedimiento de contingencia

1. Cada usuario debe disponer de una copia del procedimiento de contingencia, en aquellos aspectos que le afecten, en un lugar accesible. Asimismo, tiene que haber sido instruido acerca de las actuaciones que debe ejecutar en cada situación prevista.

2. Las situaciones en las que se produzca una contingencia deber ser registradas como una incidencia.

3. Cuando el responsable de seguridad lo estime oportuno podrá realizar simulacros de situaciones de contingencia con el fin de verificar la ejecución de las respuestas adecuadas en cada caso.

4. Los resultados no previstos de este simulacro deben registrarse como incidencias.

Artículo 46. Elementos de seguridad

1. Las ubicaciones físicas donde se encuentren los servidores de aplicaciones deberán encontrarse en áreas cerradas o áreas de seguridad.

2. La puerta de acceso a esta área deberá encontrarse permanentemente cerrada estableciéndose mecanismos para el control de accesos a la misma.

3. Estos dispositivos pueden ser sustituidos, alternativamente, por un sistema de acceso mediante códigos personales.

4. Los materiales peligrosos y/o combustibles deben almacenarse en el exterior del área y a una distancia de seguridad de la sala de ordenadores.

5. Los dispositivos de salvados de datos (cintas, cassettes, etc.) se almacenarán en armarios ignífugos, preferentemente en otros locales diferentes a las áreas de seguridad. Estos armarios estarán cerrados de forma segura.

6. Debe instalarse en el área adecuado equipamiento de seguridad tales como sistemas de extinción, detectores de humos, etc.

7. El personal externo que deba efectuar trabajos en el interior del área de seguridad debe encontrarse debidamente autorizado e identificado. El responsable del área extenderá una acreditación a favor de este personal.

8. El personal extern, no acreditat, mai romandrà a soles en l'interior de l'àrea de sistemes, sense la presència, almenys, d'una persona habilitada per a aquesta àrea.

Article 47. Supervisió d'elements de seguretat

1. El responsable de seguretat revisarà, en aquelles aplicacions del seu àmbit, que els locals i els servidors d'aplicacions al servei d'aquelles compleixen els requisits de seguretat que s'estableixen en aquestes normes.

2. En cas d'incompliment d'alguna d'aquestes, haurà de considerar aquest fet com una incidència, i com a tal registrar-se.

3. Una còpia d'aquesta incidència, addicionalment al preceptiu enviament a l'autoritat autentificadora, serà enviada el responsable de la unitat d'informàtica en què es troben adscrits els servidors d'aplicació.

II. AUTORITATS I PERSONAL

c) NOMENAMENTS, CESSAMENTS, SITUACIONS I INCIDÈNCIES

1. Administració territorial de la Generalitat Valenciana

Conselleria de Justícia i Administracions Públiques

DECRET 1/2000, d'11 de gener, del Govern Valencià, pel qual es nomenen notaris per a proveir notaries vacants a la Comunitat Valenciana. [2000/M241]

Vist, l'expedient instruït per a la provisió de notaries vacats al territori de la Comunitat Valenciana, amb motiu del concurs ordinari convocat per la Resolució de 25 d'octubre de 1999, de la Direcció General dels Registres i del Notariat, d'acord amb els articles 23, 91 al 96, i resta dels concordants del Reglament Notarial vigent, atés allò que disposa l'Estatut d'Autonomia de la Comunitat Valenciana, aprovat per la Llei Orgánica 5/1982, d'1 de juliol, a proposta del conseller de Justícia i Administracions Públiques, i amb la deliberació prèvia del Govern Valencià, en la reunió del dia 11 de gener de 2000,

DECRETE

Article únic

Són nomenats, per a proveir notaries vacants al territori de la Comunitat Valenciana, els notaris que a continuació s'allisten:

1. València, Juan Francisco Herrera García-Canturri, notari de Llíria, 3ª.
2. Torrevieja, Luis María Martínez Pertusa, notari de la Vila Joiosa, 2ª.
3. Alfafar, José Luis Micó Argilés, notari de Teruel 1ª.
4. Albocàsser, Enrique Ambrosio Martí Sanchez de León, notari oposició 1997.
5. València, Francisco José Sapena Davo, notari de Lleida, 1ª.
6. València, Fernando de la Puente de Alfaro, notari excedent 2ª.
7. Elx, Teresa de Jesús Vadillo Casero, notària de Logrosán, 3ª.
8. Llíria, Ana María Más Mayor, notària de Benaguasil, 3ª.

València, 11 de gener de 2000

El president de la Generalitat Valenciana,
EDUARDO ZAPLANA HERNÁNDEZ-SORO

El conseller de Justícia i Administracions Públiques,
SERAFÍN CASTELLANO GÓMEZ

8. El personal externo no acreditado nunca debe permanecer a solas en el interior del área de sistemas sin la presencia de al menos una persona habilitada para esta área.

Artículo 47. Supervisión de elementos de seguridad

1. El responsable de seguridad chequeará, en aquellas aplicaciones de su ámbito, que los locales y los servidores de aplicaciones al servicio de aquellas cumplen los requisitos de seguridad que se establecen en estas normas.

2. En caso de incumplimiento de alguna de las mismas, deberá considerar este hecho como una incidencia, y como tal registrarse.

3. Una copia de esta incidencia, adicionalmente al preceptivo envío a la autoridad autentificadora, será enviada al responsable de la unidad de informática a la que se encuentren adscritos los servidores de aplicación.

II. AUTORIDADES Y PERSONAL

c) NOMBRAMIENTOS, CESES, SITUACIONES E INCIDENCIAS

1. Administración territorial de la Generalitat Valenciana

Conselleria de Justicia y Administraciones Públicas

DECRETO 1/2000, de 11 de enero, del Gobierno Valenciano, por el que se nombran notarios para proveer notarías vacantes en la Comunidad Valenciana. [2000/M241]

Visto el expediente instruido para la provisión de notarías vacantes en el territorio de la Comunidad Valenciana, con motivo del concurso ordinario convocado por la Resolución de 25 de octubre de 1999, de la Dirección General de los Registros y del Notariado, de conformidad con los artículos 23, 91 al 96, y demás concordantes del Reglamento Notarial vigente, teniendo en cuenta lo dispuesto en el Estatuto de Autonomía de la Comunidad Valenciana, aprobado por la Ley Orgánica 5/1982, de 1 de julio, a propuesta del conseller de Justicia y Administraciones Públicas y previa deliberación del Gobierno Valenciano, en la reunión del día 11 de enero de 2000,

DISPONGO

Artículo único

Se nombran, para proveer las notarías vacantes en el territorio de la Comunidad Valenciana, a los notarios que a continuación se indica:

1. Valencia, a Juan Francisco Herrera García-Canturri, notario de Llíria, 3ª.
2. Torrevieja, a Luis María Martínez Pertusa, notario de Villajoyosa, 2ª.
3. Alfafar, a José Luis Micó Argilés, notario de Teruel 1ª.
4. Albocàsser, a Enrique Ambrosio Martí Sánchez de León, notario oposición 1997.
5. Valencia, a Francisco José Sapena Davo, notario de Lleida, 1ª.
6. Valencia, a Fernando de la Puente de Alfaro, notario excedente 2ª.
7. Elche, a Teresa de Jesús Vadillo Casero, notaria de Logrosán, 3ª.
8. Llíria, a Ana María Más Mayor, notaria de Benaguasil, 3ª.

Valencia, 11 de enero de 2000

El presidente de la Generalitat Valenciana,
EDUARDO ZAPLANA HERNÁNDEZ-SORO

El conseller de Justicia y Administraciones Públicas,
SERAFÍN CASTELLANO GÓMEZ