

Conselleria d'Hisenda i Administració Pública

DECRET 66/2012, de 27 d'abril, del Consell, pel qual s'estableix la política de seguretat de la informació de la Generalitat. [2012/4162]

ÍNDEX

Preàmbul
Capítol I. Naturalesa i destinataris
Article 1. Objecte
Article 2. Àmbit d'aplicació
Capítol II. Principis i obligacions
Article 3. La seguretat com a procés integral
Article 4. Gestió de riscos
Article 5. Classificació de la informació
Article 6. Separació de funcions
Article 7. Planificació i coordinació
Article 8. Accés a la informació
Article 9. Registre d'activitat
Article 10. Confidencialitat i deure de secret
Article 11. Ús d'instal·lacions i equipament
Article 12. Característiques dels sistemes d'informació
Article 13. Protecció de la informació emmagatzemada i en trànsit

Capítol III. Desenvolupament
Article 14. Desplegament
Capítol IV. Difusió, actualització i obligacions
Article 15. Publicitat, monitorització i revisió
Article 16. Obligacions del personal
Disposició addicional primera. Relacions amb tercers
Disposició addicional segona. Possibilitat d'adhesió
Disposició derogatòria única. Derogació normativa
Disposició final primera. Desplegament
Disposició final segona. Entrada en vigor

PREÀMBUL

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

La seguretat de la informació té com a objectiu protegir la informació i els servicis reduint els riscos a què estan sotmesos fins a un nivell que resulte acceptable. Dins de cada organització només els seus màxims directius tenen les competències necessàries per a fixar el dit nivell, ordenar les actuacions i habilitar els mitjans per a dur-les a terme. En este sentit, establir una política de seguretat de la informació, i fer el subsegüent repartiment de tasques i responsabilitats, són actuacions prioritàries, ja que són els dos instruments principals per al govern de la seguretat i constitueixen el marc de referència per a totes les actuacions posteriors. El present decret estableix la política de seguretat de la informació de la Generalitat, i es complementarà amb el desenvolupament de l'organització de la seguretat. Amb ambdós disposicions la Generalitat es dota de dos instruments eficaços per a millorar la seguretat de la informació sota la seua responsabilitat, sense limitar-se pel que fa a dades personals o a la que intervé en procediments d'administració electrònica.

L'article 45 de la Llei de Règim Jurídic de les Administracions Públiques i del Procediment Administratiu Comú, sota la rúbrica Incorporació de mitjans tècnics, estableix que les administracions públiques impulsaran l'ocupació i l'aplicació de les tècniques i mitjans electrònics, informàtics i telemàtics per al desenvolupament de la seua activitat i l'exercici de les seues competències.

La Llei Orgànica 15/1999, de 13 de desembre, de Protecció de Dades de Caràcter Personal, en l'article 9.1 obliga els responsables dels

Conselleria de Hacienda y Administración Pública

DECRETO 66/2012, de 27 de abril, del Consell, por el que se establece la política de seguridad de la información de la Generalitat. [2012/4162]

ÍNDICE

Preámbulo
Capítulo I. Naturaleza y destinatarios
Artículo 1. Objeto
Artículo 2. Ámbito de aplicación
Capítulo II. Principios y obligaciones
Artículo 3. La seguridad como proceso integral.
Artículo 4. Gestión de riesgos
Artículo 5. Clasificación de la información
Artículo 6. Separación de funciones
Artículo 7. Planificación y coordinación
Artículo 8. Acceso a la información
Artículo 9. Registro de actividad
Artículo 10. Confidencialidad y deber de secreto
Artículo 11. Uso de instalaciones y equipamiento
Artículo 12. Características de los sistemas de información
Artículo 13. Protección de la información almacenada y en tránsito

Capítulo III. Desarrollo
Artículo 14. Desarrollo
Capítulo IV. Difusión, actualización y obligaciones
Artículo 15. Publicidad, monitorización y revisión
Artículo 16. Obligaciones del personal
Disposición adicional primera. Relaciones con terceros
Disposición adicional segunda. Posibilidad de adhesión
Disposición derogatoria única. Derogación normativa
Disposición final primera. Desarrollo
Disposición final segunda. Entrada en vigor

PREÁMBULO

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

La seguridad de la información tiene como objetivo proteger la información y los servicios reduciendo los riesgos a los que están sometidos hasta un nivel que resulte acceptable. Dentro de cada organización sólo sus máximos directivos tienen las competencias necesarias para fijar dicho nivel, ordenar las actuaciones y habilitar los medios para llevarlas a cabo. En este sentido, establecer una política de seguridad de la información, y hacer el subsiguiente reparto de tareas y responsabilidades, son actuaciones prioritarias, puesto que son los dos instrumentos principales para el gobierno de la seguridad y constituyen el marco de referencia para todas las actuaciones posteriores. El presente decreto establece la política de seguridad de la información de la Generalitat, y se complementarà con el desarrollo de la organización de la seguridad. Con ambas disposiciones la Generalitat se dota de dos instrumentos eficaços para mejorar la seguridad de la información bajo su responsabilidad, sin limitarse a la que se refiere a datos personales o a la que interviene en procedimientos de administración electrónica.

El artículo 45 de la Ley de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, bajo la rúbrica Incorporación de medios técnicos, establece que las administraciones públicas impulsarán el empleo y aplicación de las técnicas y medios electrónicos, informáticos y telemáticos para el desarrollo de su actividad y el ejercicio de sus competencias.

La Ley Orgànica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, en su artículo 9.1 obliga a los responsables

fitxers que continguen dades personals a «adoptar les mesures d'indole tècnica i organitzatives necessàries que garantisquen la seguretat de les dades de caràcter personal i eviten la seua alteració, pèrdua, tractament o accés no autoritzat».

La Llei 11/2007, de 22 de juny, d'Accés Electrònic dels Ciutadans als Servicis Públics, en la seua part expositiva, entre altres punts, precisa que «els tècnics i els científics han posat en peu els instruments d'esta societat, però la seua generalització depèn, en gran manera, de l'impuls que reba de les administracions públiques», figurant entre els seus fins crear les condicions de confiança en l'ús dels mitjans electrònics, establint les mesures necessàries per a la preservació de la integritat dels drets fonamentals, i, en especial, els relacionats amb la intimitat i la protecció de dades de caràcter personal per mitjà de la garantia de la seguretat dels sistemes, les dades, les comunicacions i els servicis electrònics. 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, té com a finalitat la creació de les condicions necessàries de confiança en l'ús dels mitjans electrònics.

L'Esquema Nacional de Seguretat en l'àmbit de l'administració electrònica obliga els òrgans superiors de les administracions públiques a dotar-se formalment d'una política de seguretat, que haurà d'atindre's als principis bàsics i requisits mínims que s'indiquen en els capítols II i III del Reial Decret 3/2010, de 8 de gener.

La disposició final octava de la Llei 11/2007, de 22 de juny, establix que correspon al govern i a les comunitats autònomes, en l'àmbit de les seues competències respectives, dictar les disposicions necessàries per al desplegament i aplicació de l'esmentada llei.

En l'àmbit autonòmic, els antecedents normatius en esta matèria es troben en el Decret 96/1998, de 6 de juliol, del Consell, pel qual es regulen l'organització de la funció informàtica, la utilització dels sistemes d'informació i el registre de fitxers informatitzats en l'àmbit de l'administració de la Generalitat, i en el Decret 112/2008, de 25 de juliol, del Consell, pel qual es va crear la Comissió Interdepartamental per a la Modernització Tecnològica, la Qualitat i la Societat del Coneixement a la Comunitat Valenciana.

D'altra banda, la Llei 3/2010, de 5 de maig, de la Generalitat, d'Administració Electrònica de la Comunitat Valenciana, es va promulgar a l'empara de l'article 19.2 de l'Estatut d'Autonomia de la Comunitat Valenciana, que reconeix el dret d'accés dels valencians a les noves tecnologies i que la Generalitat desenvolupa polítiques actives que impulsen la formació, les infraestructures i la seua utilització, així com de l'article 49.3.16, que establix que la Generalitat té la competència exclusiva sobre el «règim de les noves tecnologies relacionades amb la societat de la informació i del coneixement».

L'article 37.4 de la Llei 3/2010, de 5 de maig, de la Generalitat, disposa que les «administracions públiques, en funció de la seua capacitat i possibilitats, aprovaran, o adoptaran per mitjà dels oportuns acords i convenis, polítiques de seguretat de la informació per a l'aplicació efectiva dels principis assenyalats en els apartats anteriors, podent promoure la constitució o incorporació als grups i centres de seguretat a què es refereix l'article 35.6 d'esta llei».

Per tot allò que s'ha exposat, en compliment del que disposa la disposició final octava de la Llei 11/2007, de 22 de juny, d'Accés Electrònic dels Ciutadans als Servicis Públics, i de l'article 37.4 de la Llei 3/2010, de 5 de maig, de la Generalitat, d'Administració Electrònica de la Comunitat Valenciana, a proposta del conseller d'Hisenda i Administració Pública, conforme amb el Consell Jurídic Consultiu de la Comunitat Valenciana i amb la deliberació prèvia del Consell, en la reunió del dia 27 d'abril de 2012,

DECRETE

CAPÍTOL I

Naturalesa i destinataris

Article 1. Objecte

El present decret té com a finalitat definir i regular la política de seguretat de la informació que s'ha d'aplicar en el tractament de la informació situada sota la responsabilitat dels diferents òrgans de l'Administració de la Generalitat i les seues entitats autònomes.

de los ficheros que contengan datos personales a «adoptar las medidas de índole técnica y organizativas necesarias que garantizan la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado».

La Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos, en su parte expositiva, entre otros extremos, precisa que «los técnicos y los científicos han puesto en pie los instrumentos de esta sociedad, pero su generalización depende, en buena medida, del impulso que reciba de las administraciones públicas», figurando entre sus fines el crear las condiciones de confianza en el uso de los medios electrónicos, estableciendo las medidas necesarias para la preservación de la integridad de los derechos fundamentales, y, en especial, los relacionados con la intimidad y la protección de datos de carácter personal por medio de la garantía de la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos. El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica, tiene como finalidad la creación de las condiciones necesarias de confianza en el uso de los medios electrónicos.

El Esquema Nacional de Seguridad en el ámbito de la administración electrónica obliga a los órganos superiores de las administraciones públicas a dotarse formalmente de una política de seguridad, que deberá atenerse a los principios básicos y requisitos mínimos que se relacionan en los capítulos II y III del Real Decreto 3/2010, de 8 de enero.

La disposición final octava de la Ley 11/2007, de 22 de junio, establece que corresponde al Gobierno y a las comunidades autónomas, en el ámbito de sus respectivas competencias, dictar las disposiciones necesarias para el desarrollo y aplicación de la citada ley.

En el ámbito autonómico, los antecedentes normativos en esta materia se encuentran en el Decreto 96/1998, de 6 de julio, del Consell, por el que se regulan la organización de la función informática, la utilización de los sistemas de información y el registro de ficheros informatizados en el ámbito de la administración de la Generalitat, y en el Decreto 112/2008, de 25 de julio, del Consell, por el que se creó la Comisión Interdepartamental para la Modernización Tecnológica, la Calidad y la Sociedad del Conocimiento en la Comunitat Valenciana.

Por otra parte, la Ley 3/2010, de 5 de mayo, de la Generalitat, de Administración Electrónica de la Comunitat Valenciana, se promulgó al amparo del artículo 19.2 del Estatut d'Autonomia de la Comunitat Valenciana, que reconoce el derecho de acceso de los valencianos a las nuevas tecnologías y a que la Generalitat desarrolle políticas activas que impulsen la formación, las infraestructuras y su utilización, así como del artículo 49.3.16, que establece que la Generalitat tiene competencia exclusiva sobre el «régimen de las nuevas tecnologías relacionadas con la sociedad de la información y del conocimiento».

El artículo 37.4 de la Ley 3/2010, de 5 de mayo, de la Generalitat, dispone que «las administraciones públicas, en función de su capacidad y posibilidades, aprobarán, o adoptarán mediante los oportunos acuerdos y convenios, políticas de seguridad de la información para la aplicación efectiva de los principios señalados en los apartados anteriores, pudiendo promover la constitución o incorporación a los grupos y centros de seguridad a los que se refiere el artículo 35.6 de esta ley».

Por lo expuesto, en cumplimiento de lo dispuesto en la disposición final octava de la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos, y del artículo 37.4 de la Ley 3/2010, de 5 de mayo, de la Generalitat, de Administración Electrónica de la Comunitat Valenciana, a propuesta del conseller de Hacienda y Administración Pública, conforme con el Consell Jurídic Consultiu de la Comunitat Valenciana y previa deliberación del Consell, en la reunión del día 27 de abril de 2012,

DECRETO

CAPÍTULO I

Naturaleza y destinatarios

Artículo 1. Objeto

El presente decreto tiene por objeto definir y regular la política de seguridad de la información que se ha de aplicar en el tratamiento de la información situada bajo la responsabilidad de los distintos órganos de la administración de la Generalitat y sus entidades autónomas.

Article 2. Àmbit d'aplicació

La política de seguretat regulada en el present decret haurà d'aplicar-se a tota la informació sota la responsabilitat de l'Administració de la Generalitat i les seues entitats autònomes, així com al tractament de què pugua ser objecte. Esta consideració no es limita a les dades de caràcter personal i és independent que el tractament siga manual o automatitzat.

CAPÍTOL II *Principis i obligacions*

Article 3. La seguretat com a procés integral

1. La seguretat de la informació és el resultat d'un procés que depèn de tots i cada un dels elements humans, tècnics, materials i organitzatius que intervenen en el tractament. Els que participen en qualsevol fase del tractament hauran de respondre, en la mesura de les seues responsabilitats, de la seguretat i bon ús de la informació. De manera especial, hauran de col·laborar en la prevenció, detecció i control dels riscos derivats d'actuacions negligents, ignorància de les normes, fallades tècniques, d'organització o de coordinació, o instruccions inadequades.

2. La Generalitat, a través dels diferents agents amb responsabilitats específiques en matèria de seguretat de la informació, s'encarregarà de proporcionar els canals de participació adequats que facen efectiva la col·laboració mencionada en l'apartat anterior. De la mateixa manera, la Generalitat s'ocuparà de mantindre permanentment informats, a tots els destinataris d'esta política, del propòsit i contingut d'esta, així com dels documents que la despleguen i dels canals de participació habilitats.

3. El procés de gestió de la seguretat de la informació haurà d'estar sotmés a monitorització, control i millora continus per a confirmar la seua eficàcia davant de la constant evolució dels riscos i dels sistemes de protecció.

Article 4. Gestió de riscos

1. El govern i la gestió de la seguretat de la informació es guiaran pels resultats dels processos d'anàlisi i gestió de riscos.

2. Els responsables de seguretat de la informació elaboraran un informe anual sobre l'estat de la seguretat, els riscos previsibles i els plans d'actuació recomanats. Estos informes s'elevaran als responsables de la informació i, si és el cas, als responsables de tractament, els quals fixaran el nivell de risc acceptable i ordenaran les actuacions oportunes.

3. La reducció dels nivells de risc es realitzarà per mitjà de l'aplicació de controls. La selecció i aplicació dels controls ponderaran el valor dels actius amb els nivells de risc i el cost de la seguretat.

4. Els controls hauran de ser eficaços abans, durant o després que ocorrega un incident de seguretat. El seu objectiu és evitar que succeïsquen incidències i controlar els danys si és que finalment arriben a produir-se.

5. L'anàlisi i la gestió de riscos hauran d'estar presents en totes les fases del cicle de vida de les aplicacions i servicis relacionats amb el tractament de la informació, començant per la de l'estudi de viabilitat.

6. La selecció i l'aplicació dels controls de seguretat, així com l'avaluació de la seua eficiència, hauran de tindre's en compte durant el disseny, construcció, contractació, adquisició, explotació, tancament, terminació, cancel·lació o alienació de les aplicacions i servicis mencionats.

7. Els òrgans competents de la Generalitat valoraran en les contractacions aquelles empreses, productes i servicis que puguen acreditar un nivell de qualitat o seguretat. El compliment d'un nivell mínim determinat podrà ser un requisit imprescindible.

Article 5. Classificació de la informació

Els actius d'informació hauran d'estar inventariats i classificats. El nivell de protecció i les mesures a aplicar es basaran en el resultat de la dita classificació.

Artículo 2. Ámbito de aplicación

La política de seguridad regulada en el presente decreto deberá aplicarse a toda la información bajo la responsabilidad de la administración de la Generalitat y sus entidades autónomas, así como al tratamiento de lo que pueda ser objeto. Esta consideración no se limita a los datos de carácter personal y es independiente de que el tratamiento sea manual o automatizado.

CAPÍTULO II *Principios y obligaciones*

Artículo 3. La seguridad como proceso integral

1. La seguridad de la información es el resultado de un proceso que depende de todos y cada uno de los elementos humanos, técnicos, materiales y organizativos que intervienen en el tratamiento. Quienes participan en cualquier fase del tratamiento deberán responder, en la medida de sus responsabilidades, de la seguridad y buen uso de la información. De manera especial, deberán colaborar en la prevención, detección y control de los riesgos derivados de actuaciones negligentes, ignorancia de las normas, fallos técnicos, de organización o de coordinación, o instrucciones inadecuadas.

2. La Generalitat, a través de los distintos agentes con responsabilidades específicas en materia de seguridad de la información, se encargará de proporcionar los canales de participación adecuados que hagan efectiva la colaboración mencionada en el apartado anterior. Del mismo modo, la Generalitat se ocupará de mantener permanentemente informados, a todos los destinatarios de esta política, del propósito y contenido de la misma, así como de los documentos que la desarrollan y de los canales de participación habilitados.

3. El proceso de gestión de la seguridad de la información deberá estar sometido a monitorización, control y mejora continuos para confirmar su eficacia ante la constante evolución de los riesgos y de los sistemas de protección.

Artículo 4. Gestión de riesgos

1. El gobierno y la gestión de la seguridad de la información se guiarán por los resultados de los procesos de análisis y gestión de riesgos.

2. Los responsables de seguridad de la información elaborarán un informe anual sobre el estado de la seguridad, los riesgos previsibles y los planes de actuación recomendados. Estos informes se elevarán a los responsables de la información y, en su caso, a los responsables de tratamiento, quienes fijarán el nivel de riesgo acceptable y ordenarán las actuaciones oportunas.

3. La reducción de los niveles de riesgo se realizará mediante la aplicación de controles. La selección y aplicación de los controles ponderarán el valor de los activos con los niveles de riesgo y el coste de la seguridad.

4. Los controles deberán ser eficaces antes, durante o después de que ocurra un incidente de seguridad. Su objetivo es evitar que sucedan incidencias y controlar los daños si es que finalmente llegan a producirse.

5. El análisis y la gestión de riesgos deberán estar presentes en todas las fases del ciclo de vida de las aplicaciones y servicios relacionados con el tratamiento de la información, empezando por la del estudio de viabilidad.

6. La selección y aplicación de los controles de seguridad, así como la evaluación de su eficiencia, deberán tenerse en cuenta durante el diseño, construcción, contratación, adquisición, explotación, cierre, terminación, cancelación o enajenación de las aplicaciones y servicios mencionados.

7. Los órganos competentes de la Generalitat valorarán en las contrataciones aquellas empresas, productos y servicios que puedan acreditar un nivel de calidad o seguridad. El cumplimiento de un nivel mínimo determinado podrá ser un requisito imprescindible.

Artículo 5. Clasificación de la información

Los activos de información deberán estar inventariados y clasificados. El nivel de protección y las medidas a aplicar se basarán en el resultado de dicha clasificación.

Article 6. Separació de funcions

La seguretat de la informació exigix un repartiment de tasques i responsabilitats amb una clara separació de funcions. En particular, s'haurà de mantindre una clara distinció entre els tres papers següents: responsables de la informació, responsables del servei i responsables de seguretat, que seran definits en l'esquema organitzatiu.

Article 7. Planificació i coordinació

1. Els objectius a mig termini per a la millora de la seguretat de la informació s'explicitaran en els corresponents plans estratègics. Estos plans contindran una descripció de les línies d'actuació previstes, projectes, indicadors de compliment i de progrés, així com mètriques per a avaluar l'efectivitat. Estos plans es revisaran anualment tenint en compte els resultats de les auditories i de les avaluacions de riscos. Els plans estratègics, els informes de seguiment i les revisions anuals se sotmetran a l'aprovació dels responsables de la informació o dels responsables de tractament, segons corresponga.

2. La coordinació entre tots els agents de què depén la seguretat de la informació ha de formar part de totes les iniciatives i actuacions. La Generalitat habilitarà els mitjans tècnics necessaris per a facilitar esta coordinació. Els responsables de seguretat actuaran de manera coordinada en l'aplicació i control de les mesures de seguretat.

3. Les empreses de servicis, organitzacions i entitats amb accés a informació situada sota la responsabilitat de la Generalitat hauran de nomenar un responsable de seguretat que actue com a interlocutor vàlid als efectes de la coordinació en esta matèria.

Article 8. Accés a la informació

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

2. Els responsables de la informació hauran de nomenar un responsable d'accés per a cada actiu d'informació, qui al seu torn podrà nomenar delegats on es realitze tractament.

3. Cada intent d'accés haurà de quedar registrat amb el suficient nivell de detall. Els responsables dels accessos revisaran i informaran estos registres.

Article 9. Registre d'activitat

Les actuacions de les persones, en tant que formen part de determinat tractament d'informació, podran ser registrades en compliment de les exigències legals de traçabilitat. També podran ser-ho per a monitoritzar el compliment de la present política. En tot cas, el registre d'estes actuacions es realitzarà preservant els drets dels afectats i respectant la normativa laboral aplicable.

Article 10. Confidencialitat i deure de secret

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

Article 11. Ús d'instal·lacions i d'equipament

1. La Generalitat dotarà els llocs de treball amb l'equipament informàtic i de comunicacions necessari per a l'exercici de les funcions encomanades. Estos equips no estan destinats a l'ús personal.

2. L'equipament mencionat en l'apartat anterior no podrà utilitzar-se per a activitats il·lícites o irregulars, o que afecten negativament el funcionament de l'Administració o siguen contràries als interessos d'esta.

3. La instal·lació o la utilització d'elements de maquinari o programari aliens que formen part de la configuració del lloc de treball requeriran una autorització prèvia per part de l'òrgan competent en matèria de tecnologies de la informació que corresponga.

4. Les infraestructures informàtiques i de comunicacions que no formen part dels llocs de treball hauran d'ubicar-se en àrees separades, d'accés restringit i suficientment protegides d'acord amb la naturalesa de la informació i dels servicis en què intervinguen.

Artículo 6. Separación de funciones

La seguridad de la información exige un reparto de tareas y responsabilidades con una clara separación de funciones. En particular, se deberá mantener una clara distinción entre los tres siguientes papeles: responsables de la información, responsables del servicio y responsables de seguridad, que serán definidos en el esquema organizativo.

Artículo 7. Planificación y coordinación

1. Los objetivos a medio plazo para la mejora de la seguridad de la información se explicitarán en los correspondientes planes estratégicos. Estos planes contendrán una descripción de las líneas de actuación previstas, proyectos, indicadores de cumplimiento y de progreso, así como métricas para evaluar la efectividad. Estos planes se revisarán anualmente teniendo en cuenta los resultados de las auditorías y de las evaluaciones de riesgos. Los planes estratégicos, los informes de seguimiento y las revisiones anuales se someterán a la aprobación de los responsables de la información o de los responsables de tratamiento, según corresponda.

2. La coordinación entre todos los agentes de los que depende la seguridad de la información debe formar parte de todas las iniciativas y actuaciones. La Generalitat habilitará los medios técnicos necesarios para facilitar esa coordinación. Los responsables de seguridad actuarán de manera coordinada en la aplicación y control de las medidas de seguridad.

3. Las empresas de servicios, organizaciones y entidades con acceso a información situada bajo la responsabilidad de la Generalitat deberán nombrar un responsable de seguridad que actúe como interlocutor válido a los efectos de la coordinación en esa materia.

Artículo 8. Acceso a la información

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

2. Los responsables de la información deberán nombrar un responsable de acceso para cada activo de información, quien a su vez podrá nombrar delegados donde se realice tratamiento.

3. Cada intento de acceso deberá quedar registrado con el suficiente nivel de detalle. Los responsables de los accesos revisarán e informarán estos registros.

Artículo 9. Registro de actividad

Las actuaciones de las personas, en tanto que formen parte de determinado tratamiento de información, podrán ser registradas en cumplimiento de las exigencias legales de trazabilidad. También podrán serlo para monitorizar el cumplimiento de la presente política. En todo caso, el registro de tales actuaciones se realizará preservando los derechos de los afectados y respetando la normativa laboral aplicable.

Artículo 10. Confidencialidad y deber de secreto

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

Artículo 11. Uso de instalaciones y equipamiento

1. La Generalitat dotará los puestos de trabajo con el equipamiento informático y de comunicaciones necesario para el desempeño de las funciones encomendadas. Dichos equipos no están destinados al uso personal.

2. El equipamiento mencionado en el apartado anterior no podrá utilizarse para actividades ilícitas o irregulares, o que afecten negativamente al funcionamiento de la Administración o sean contrarias a los intereses de ésta.

3. La instalación o utilización de elementos hardware o software ajenos a los que forman parte de la configuración del puesto de trabajo requerirán una autorización previa por parte del órgano competente en materia de tecnologías de la información que corresponda.

4. Las infraestructuras informáticas y de comunicaciones que no formen parte de los puestos de trabajo deberán ubicarse en áreas separadas, de acceso restringido y suficientemente protegidas de acuerdo con la naturaleza de la información y de los servicios en que intervengan.

Article 12. Característiques dels sistemes d'informació

1. Els sistemes d'informació proporcionaran la funcionalitat estrictament necessària per a complir els propòsits declarats, i cap més.

2. L'ús ordinari dels sistemes d'informació ha de ser senzill i segur, de manera que una utilització insegura requerisca un acte conscient per part de l'usuari.

3. Les funcions d'operació, administració, manteniment i registre d'activitat seran les mínimes necessàries, hauran d'estar descrites i documentades i subjectes a controls estrictes.

Article 13. Protecció de la informació emmagatzemada i en trànsit

1. La Generalitat, a través dels distints agents amb responsabilitats específiques en matèria de seguretat de la informació, establirà les condicions per a la protecció en el tractament d'informació fora dels seus locals i sistemes.

2. La Generalitat garantirà, de la mateixa manera que l'apartat anterior, la conservació i la recuperació de la informació mentre perdure la seua vigència.

3. La informació en suport no electrònic que haja sigut causa o conseqüència directa de tractament automatitzat d'informació haurà de protegir-se amb el mateix grau de seguretat que esta.

CAPÍTOL III
Desenrotllament

Article 14. Desplegament

1. Esta política es desplegarà en un conjunt de documents l'objectiu dels quals és facilitar que el tractament d'informació es realitze d'acord amb els objectius i principis exposats en els articles anteriors.

2. Els documents mencionats en el punt anterior hauran d'abordar, almenys, els aspectes següents:

- a) Condicions per a l'accés a la informació.
- b) Ús de l'equipament informàtic i de comunicacions.
- c) Gestió d'incidents i problemes.
- d) Continuitat d'operacions.
- e) Seguretat amb tercers.
- f) Classificació i tractament de la informació.
- g) Anàlisi i gestió de riscos.
- h) Seguretat física i del personal.
- i) Prevenció de virus i codi maliciós.
- j) Cicle de vida dels sistemes d'informació.
- k) Millora contínua. Nivells de maduresa.
- l) Elaboració, publicació i revisió de la política de seguretat de la informació i dels documents complementaris.

3. Els documents mencionats en el punt 1 estaran agrupats en tres col·leccions: normes, procediments i guies de bones pràctiques.

4. Les normes proporcionaran un primer nivell de concreció; cada una d'estes estarà dirigida a un tipus d'activitat determinat. Els procediments descriuran la seqüència concreta de passos per a completar una tasca. Les guies de bones pràctiques oferiran recomanacions sobre com actuar en situacions específiques.

Les normes i els procediments tindran caràcter obligatori. Les possibles excepcions hauran de justificar-se.

CAPÍTOL IV
Difusió, actualització i obligacions

Article 15. Publicitat, monitorització i revisió

1. La Generalitat disposarà dels mitjans per a publicar, donar a conèixer i facilitar el compliment d'esta política i dels documents que la despleguen, així com per a verificar la seua aplicació i efectivitat. Així mateix, habilitarà canals de participació que permeten, als destinataris d'esta política i dels documents complementaris, participar en la seua revisió i millora.

2. Els responsables de seguretat inclouran en les seues memòries anuals un apartat sobre el grau de compliment i eficàcia d'esta normativa i un altre proposant accions de millora. Estes memòries es presentaran al responsable en matèria de seguretat de la informació que corresponga perquè aprobe les actuacions oportunes.

Artículo 12. Características de los sistemas de información

1. Los sistemas de información proporcionarán la funcionalidad estrictamente necesaria para cumplir los propósitos declarados, y ninguna más.

2. El uso ordinario de los sistemas de información ha de ser sencillo y seguro, de forma que una utilización insegura requiera de un acto consciente por parte del usuario.

3. Las funciones de operación, administración, mantenimiento y registro de actividad serán las mínimas necesarias, deberán estar descritas y documentadas y sujetas a controles estrictos.

Artículo 13. Protección de la información almacenada y en tránsito

1. La Generalitat, a través de los distintos agentes con responsabilidades específicas en materia de seguridad de la información, establecerá las condiciones para la protección en el tratamiento de información fuera de sus locales y sistemas.

2. La Generalitat garantizará, del mismo modo que el apartado anterior, la conservación y recuperación de la información mientras perdure su vigencia.

3. La información en soporte no electrónico que haya sido causa o consecuencia directa de tratamiento automatizado de información deberá protegerse con el mismo grado de seguridad que ésta.

CAPÍTULO III
Desarrollo

Artículo 14. Desarrollo

1. La presente 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 los artículos anteriores.

2. Los documentos mencionados en el punto anterior deberán abordar, al menos, los siguientes aspectos:

- a) Condiciones para el acceso a la información.
- b) Uso del equipamiento informático y de comunicaciones.
- c) Gestión de incidentes y problemas.
- d) Continuidad de operaciones.
- e) Seguridad con terceros.
- f) Clasificación y tratamiento de la información.
- g) Análisis y gestión de riesgos.
- h) Seguridad física y del personal.
- i) Prevención de virus y código malicioso.
- j) Ciclo de vida de los sistemas de información.
- k) Mejora continua. Niveles de madurez.
- l) Elaboración, publicación y revisión de la política de seguridad de la información y de los documentos complementarios.

3. Los documentos mencionados en el punto 1 estarán agrupados en tres colecciones: normas, procedimientos y guías de buenas prácticas.

4. Las normas proporcionarán un primer nivel de concreción; cada una de ellas estará dirigida a un tipo de actividad determinado. Los procedimientos describirán la secuencia concreta de pasos para completar una tarea. Las guías de buenas prácticas ofrecerán recomendaciones sobre cómo actuar en situaciones específicas.

Las normas y los procedimientos tendrán carácter obligatorio. Las posibles excepciones deberán justificarse.

CAPÍTULO IV
Difusión, actualización y obligaciones

Artículo 15. Publicidad, monitorización y revisión

1. La Generalitat dispondrá los medios para publicar, dar a conocer y facilitar el cumplimiento de esta política y de los documentos que la desarrollan, así como para verificar su aplicación y efectividad. Asimismo, habilitará canales de participación que permitan, a los destinatarios de esta política y de los documentos complementarios, participar en su revisión y mejora.

2. Los responsables de seguridad incluirán en sus memorias anuales un apartado sobre el grado de cumplimiento y eficacia de esta normativa y otro proponiendo acciones de mejora. Estas memorias se presentarán al responsable en materia de seguridad de la información que corresponda para que apruebe las actuaciones oportunas.

Article 16. Obligacions del personal

1. La política de seguretat té caràcter obligatori per a tot el personal al servici de l'Administració de la Generalitat i les seues entitats autònomes, especialment per als qui participen en el tractament d'informació o tinguen accés als locals on es custodie la informació o es realitze el seu tractament.

2. Les circumstàncies exposades en el paràgraf anterior són independents del tipus de relació jurídica o laboral que es mantinga amb l'administració de la Generalitat i les seues entitats autònomes. Quan el personal afectat per alguna de les condicions indicades estiga contractat per una empresa de servicis o pertanga a alguna entitat col·laboradora, el compliment del que disposa esta política s'inclourà en els contractes o convenis que regulen la dita relació. Les subcontractacions hauran de comptar amb l'autorització expressa del responsable de la informació i en cap cas eximiran del compliment d'esta política.

3. L'incompliment de la política de seguretat expressada en este decret podrà tindre conseqüències disciplinàries, d'acord amb el règim sancionador aplicable en cada cas, sense perjudi d'altres responsabilitats en què es puga incórrer.

DISPOSICIONS ADDICIONALS

Primera. Relacions amb tercers

Els contractes o convenis a què es referix l'article 16.2 de la presente disposició que se subscriuen a partir de l'entrada en vigor d'este decret hauran d'incloure una clàusula de compliment d'esta política, juntament amb un procediment de verificació adequat. Els contractes i convenis firmats amb anterioritat a esta data seran objecte de revisió en el mateix sentit.

Segona. Possibilitat d'adhesió

La resta del sector públic valencià podrà aplicar esta política de seguretat quan així ho establisquen les seues normes internes de funcionament.

DISPOSICIÓ DEROGATÒRIA

Única. Derogació normativa

Queda derogada l'Orde de 3 de desembre de 1999, de la Conselleria de Justícia i Administració Pública, per la qual es va aprovar el Reglament Tècnic de Mesures de Seguretat per a l'Aprovació i Homologació d'Aplicacions i Mitjans de Tractament Automatitzat de la Informació, en tot el que s'opose al present decret.

Queden derogades totes les disposicions del mateix rang o inferior que s'oposen al que disposa el present decret.

DISPOSICIONS FINALS

Primera. Desplegament

Es faculta el conseller o la consellera amb competències horitzontals de la Generalitat en matèria de tecnologies de la informació i comunicació per a dictar totes les disposicions que exigisca l'aplicació i execució d'este decret.

Es faculta el conseller o la consellera amb competències en matèria de sanitat i salut pública perquè desplegue les disposicions necessàries per a establir l'organització de la seguretat de la informació en el seu àmbit de competència.

Segona. Entrada en vigor

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

València, 27 d'abril de 2012

El president de la Generalitat,
ALBERTO FABRA PART

El conseller de Hisenda i Administració Pública,
JOSÉ MANUEL VELA BARGUES

Artículo 16. Obligaciones del personal

1. La política de seguridad tiene carácter obligatorio para todo el personal al servicio de la Administración de la Generalitat y sus entidades autónomas, especialmente para quienes participan en el tratamiento de información o tengan acceso a los locales donde se custodie la información o se realice su tratamiento.

2. Las circunstancias expuestas en el párrafo anterior son independientes del tipo de relación jurídica o laboral que se mantenga con la administración de la Generalitat y sus entidades autónomas. Cuando el personal afectado por alguna de las condiciones indicadas esté contratado por una empresa de servicios o pertenezca a alguna entidad colaboradora, el cumplimiento de lo dispuesto en esta política se incluirá en los contratos o convenios que regulen dicha relación. Las subcontractaciones deberán contar con la autorización expresa del responsable de la información y en ningún caso eximirán del cumplimiento de esta política.

3. El incumplimiento de la política de seguridad expresada en este decreto podrá tener consecuencias disciplinarias, de acuerdo con el régimen sancionador aplicable en cada caso, sin perjuicio de otras responsabilidades en que se pudiera incurrir.

DISPOSICIONES ADICIONALES

Primera. Relaciones con terceros

Los contratos o convenios a los que se refiere el artículo 16.2 de la presente disposición que se suscriban a partir de la entrada en vigor de este decreto deberán incluir una cláusula de cumplimiento de esta política, junto con un procedimiento de verificación adecuado. Los contratos y convenios firmados con anterioridad a esa fecha serán objeto de revisión en el mismo sentido.

Segunda. Posibilidad de adhesión

El resto del sector público valenciano podrá aplicar esta política de seguridad cuando así lo establezcan sus normas internas de funcionamiento.

DISPOSICIÓ DEROGATORIA

Única. Derogación normativa

Queda derogada la Orden de 3 de diciembre de 1999, de la Conselleria de Justicia y Administración Pública, por la que se aprobó el Reglamento Técnico de Medidas de Seguridad para la Aprobación y Homologación de Aplicaciones y Medios de Tratamiento Automatizado de la Información, en todo lo que se oponga al presente decreto.

Quedan derogadas cuantas disposiciones de igual o inferior rango se opongan a lo dispuesto en el presente decreto.

DISPOSICIONES FINALES

Primera. Desarrollo

Se faculta al conseller o la consellera con competencias horizontales de la Generalitat en materia de tecnologías de la información y comunicación para dictar cuantas disposiciones exija la aplicación y ejecución de este decreto.

Se faculta al conseller o la consellera con competencias en materia de sanidad y salud pública para que desarrolle las disposiciones necesarias para establecer la organización de la seguridad de la información en su ámbito de competencia.

Segunda. Entrada en vigor

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

València, 27 de abril de 2012

El president de la Generalitat,
ALBERTO FABRA PART

El conseller de Hacienda y Administración Pública,
JOSÉ MANUEL VELA BARGUES