Conselleria d'Hisenda i Administració Pública

DECRET 130/2012, de 24 d'agost, del Consell, pel qual s'establix l'organització de la seguretat de la informació de la Generalitat. [2012/8152]

Índex

Preàmbul
Capítol I. Disposicions preliminars
Article 1. Objecte
Article 2. Àmbit d'aplicació
Article 3. Principi general d'actuació
Article 4. Definicions
Capítol II. Estructura organitzativa
Article 5. Estructura
Article 6. Organització de la seguretat de la informació
Capítol III. L'organització de la seguretat de la informació
Article 7. Responsable de la Informació
Article 8. Comité de Seguretat de la Informació
Article 9. Responsable dels Fitxers de Dades de Caràcter Personal
Article 10. Responsable del Servici
Article 11. Responsable de Seguretat de la Informació
Article 12. Responsable de Seguretat dels Fitxers de Dades de Caràcter Personal
Article 13. Responsable del Sistema
Article 14. Administradors de la Seguretat del Sistema
Article 15. Administradors de la Seguretat dels Fitxers de Dades de Caràcter Personal
Disposició derogatòria única. Derogació normativa
Disposició final primera. Nomenaments
Disposició final segona. Entrada en vigor
Annex. Glossari de termes

PREÀMBUL

La informació constituïx un actiu de primer orde per a la Generalitat des del moment que resulta essencial per a la prestació de gran part dels seus servicis. 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 vénen acompanyades de nous riscos i, per tant, és necessari introduir mesures específiques per a protegir tant la informació com els servicis que depenguen d'esta.

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 este nivell, ordenar les actuacions i habilitar els mitjans per a portar-les a cap. 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 constituïxen el marc de referència per a totes les actuacions posteriors.

L'objecte de la present disposició és establir el marc organitzatiu de la seguretat de la informació, i complementar al Decret 66/2012, de 27 d'abril, del Consell, pel qual s'establix la política de seguretat de la informació de la Generalitat, en l'àmbit de l'Administració de la Generalitat i de les seues entitats autònomes, a excepció de l'organització de seguretat que afecta la conselleria amb competències en sanitat i l'Agència Valenciana de Salut, ja que, donada l'especialitat de la regulació de la informació de què disposen, s'ha considerat oportú que la seua organització en matèria de seguretat de la informació s'aprove per mitjà d'un instrument normatiu específic.

La Llei Orgànica 15/1999, de 13 de desembre, de Protecció de Dades de Caràcter Personal (d'ara en avant, LOPD), té com a objecte garantir i protegir, en allò que concernix al tractament de les dades per-

Conselleria de Hacienda y Administración Pública

DECRETO 130/2012, de 24 de agosto, del Consell, por el que se establece la organización de la seguridad de la información de la Generalitat. [2012/8152]

Índice

Preámbulo
Capítulo I. Disposiciones preliminares
Artículo 1. Objeto
Artículo 2. Ámbito de aplicación
Artículo 3. Principio general de actuación
Artículo 4. Definiciones
Capítulo II. Estructura organizativa
Artículo 5. Estructura
Artículo 6. Organización de la seguridad de la información
Capítulo III. La organización de la seguridad de la información
Artículo 7. Responsable de la información
Artículo 8. Comité de Seguridad de la Información
Artículo 9. Responsable de los ficheros de datos de carácter personal
Artículo 10. Responsable del servicio
Artículo 11. Responsable de seguridad de la información
Artículo 12. Responsable de seguridad de los ficheros de datos de carácter personal
Artículo 13. Responsable del sistema
Artículo 14. Administradores de la seguridad del sistema
Artículo 15. Administradores de la seguridad de los ficheros de datos de carácter personal
Disposición derogatoria única. Derogación normativa
Disposición final primera. Nombramientos
Disposición final segunda. Entrada en vigor
Anexo. Glosario de términos

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 dependan 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 aceptable. 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 objeto de la presente disposición es establecer el marco organizativo de la seguridad de la información, complementando al Decreto 66/2012, de 27 de abril, del Consell, por el que se establece la política de seguridad de la información de la Generalitat, en el ámbito de la Administración de la Generalitat y de sus entidades autónomas, a excepción de la organización de seguridad que afecta a la conselleria con competencias en sanidad y a la Agència Valenciana de Salut ya que, dada la especialidad de la regulación de la información de que disponen, se ha considerado oportuno que su organización en materia de seguridad de la información se apruebe mediante un instrumento normativo específico.

La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante, LOPD), tiene como objeto garantizar y proteger, en lo que concierne al tratamiento de los datos

sonals, les llibertats públiques i els drets fonamentals de les persones físiques i especialment del seu honor i intimitat personal i familiar. El seu article 9.1 disposa que «el responsable del fitxer, i, si és el cas, l'encarregat del tractament hauran d'adoptar les mesures d'índole 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, tenint en compte l'estat de la tecnologia, la naturalesa dels dades emmagatzemades i els riscos a què estan exposats, ja provinguen de l'acció humana o del medi físic o natural».

El Reial Decret 1720/2007, de 21 de desembre, pel qual s'aprova el Reglament de desplegament de la Llei Orgànica 15/1999, de 13 de desembre, de Protecció de Dades de Caràcter Personal, establix les mesures de seguretat mínimes que han d'aplicar-se als fitxers automatitzats i no automatitzats que continguen dades de caràcter personal, entre les quals s'inclou el nomenament d'una sèrie de figures amb responsabilitats específiques.

La Llei 11/2007, de 22 de juny, d'Accés Electrònic dels Ciutadans als Servicis Públics, té entre els seus fins la creació de les condicions de confiança en l'ús dels mitjans electrònics per mitjà de l'establiment de 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. En la seua disposició final octava esta llei 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 la dita llei.

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, desenrotlla la Llei 11/2007, de 22 de juny, i fixa una sèrie de requisits mínims que han de concretar-se en el corresponent pla d'adequació. Entre tals requisits estan l'aprovació formal de la política de seguretat i l'organització de la seguretat.

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 crea la Comissió Interdepartamental per a la Modernització Tecnològica, la Qualitat i la Societat del Coneixement a la Comunitat Valenciana.

D'altra banda, és imprescindible citar també la Llei 3/2010, de 5 de maig, de la Generalitat, d'Administració Electrònica de la Comunitat Valenciana, que 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 desenrotlle polítiques actives que impulsen la formació, les infraestructures i la seua utilització, així com l'article 49.3.16a que establix que la Generalitat té la competència exclusiva sobre el «règim de les noves tecnologies relacionades amb els servicis d'informació i del coneixement». L'article 37.4 de la Llei 3/2010 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, i es podran promoure la constitució o incorporació als grups i centres de seguretat a què es referix l'article 35.6 d'esta llei».

La Llei 3/2005, de 15 de juny, de la Generalitat, d'Arxius, té com a objecte regular el Sistema Arxivístic Valencià i establir els drets i obligacions relatives al patrimoni documental, i en l'article 6.3 promou que la preservació dels documents electrònics es realitzarà de manera que es garantisca que els documents romanen complets, tant en el seu contingut com en la seua estructura i el seu context; fiables, quan puguen continuar i donar fe del contingut; autèntics, en quant que originals que no han patit alteració en les eventuals migracions; i accessibles, quant a la seua localització i llegibilitat. L'article 9 d'esta llei establix que l'òrgan directiu del Sistema Arxivístic Valencià tindrà competència sobre «la supervisió tècnica dels projectes de construcció i equipament dels arxius de la Comunitat Valenciana que formen part del Sistema Arxivístic Valencià».

Per tot això 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,

personales, las libertades públicas y los derechos fundamentales de las personas físicas y especialmente de su honor e intimidad personal y familiar. Su artículo 9.1 dispone que «el responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural».

El Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, establece las medidas de seguridad mínimas que deben aplicarse a los ficheros automatizados y no automatizados que contengan datos de carácter personal, entre las que se incluye el nombramiento de una serie de figuras con responsabilidades específicas.

La Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos, tiene entre sus fines la creación de las condiciones de confianza en el uso de los medios electrónicos mediante el establecimiento de 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. En su disposición final octava esta Ley 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 dicha Ley.

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, desarrolla la Ley 11/2007, de 22 de junio, y fija una serie de requisitos mínimos que deben concretarse en el correspondiente plan de adecuación. Entre tales requisitos están la aprobación formal de la política de seguridad y la organización de la seguridad.

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 crea la Comisión Interdepartamental para la Modernización Tecnológica, la Calidad y la Sociedad del Conocimiento en la Comunitat Valenciana.

Por otra parte, es imprescindible citar también la Ley 3/2010, de 5 de mayo, de la Generalitat, de Administración Electrónica de la Comunitat Valenciana, que 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 el artículo 49.3.16ª que establece que la Generalitat tiene la competencia exclusiva sobre el «régimen de las nuevas tecnologías relacionadas con los servicios de información y del conocimiento». El artículo 37.4 de la Ley 3/2010 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».

La Ley 3/2005, de 15 de junio, de la Generalitat, de Archivos, tiene por objeto regular el Sistema Archivístico Valenciano y establecer los derechos y obligaciones relativas al patrimonio documental, y en su artículo 6.3 promueve que la preservación de los documentos electrónicos se realizará de forma que se garantice que los documentos permanecen completos, tanto en su contenido como en su estructura y su contexto; fiables, en cuanto puedan seguir dando fe del contenido; auténticos, en cuanto que originales que no han sufrido alteración en las eventuales migraciones; y accesibles, en cuanto a su localización y legibilidad. El artículo 9 de esta Ley establece que el órgano directivo del Sistema Archivístico Valenciano tendrá competencia sobre «la supervisión técnica de los proyectos de construcción y equipamiento de los archivos de la Comunitat Valenciana que formen parte del Sistema Archivístico Valenciano».

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

trònic 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, i amb la deliberació prèvia del Consell, en la reunió del dia 24 d'agost de 2012,

DECRETE

CAPÍTOL I
Disposicions preliminars

Article 1. Objecte

L'objecte d'este decret és establir el repartiment de funcions i responsabilitats en matèria de seguretat de la informació.

Article 2. Àmbit d'aplicació

L'organització de la seguretat regulada en el present decret és aplicable a les conselleries de la Generalitat, així com a les seues entitats autònomes dependents, a les quals es referix l'article 5.1 del Text Refós de la Llei d'Hisenda Pública de la Generalitat, i s'exceptua la conselleria amb competències en sanitat i l'Agència Valenciana de Salut.

Article 3. Principi general d'actuació

La seguretat de la informació depén de totes les persones que participen en el seu tractament i compromet a totes les que integren l'organització. Tot el personal inclòs en l'àmbit d'aplicació del present decret, que participe en el tractament d'informació, inclosos empleats, subcontractistes i tercers, es comprometen a donar un ús correcte a tots els actius que requerisquen per al desenrotllament de les seues funcions, a respectar les mesures de seguretat que s'establisquen i a notificar com més prompte millor als responsables que corresponga dels esdeveniments i punts dèbils de la seguretat de la informació que detecte, de manera que puguen emprendre's les accions oportunes.

Article 4. Definicions

Als efectes previstos en este decret, les definicions, paraules, expressions i termes han de ser entesos en el sentit indicat en el glossari de termes inclòs en l'annex.

CAPÍTOL II
Estructura organitzativa

Article 5. Estructura

L'estructura organitzativa de la seguretat de la informació agrupa els agents les funcions i responsabilitats dels quals comprenen tota l'Administració de la Generalitat i les seues entitats autònomes, i s'exceptua la conselleria amb competències en sanitat i l'Agència Valenciana de Salut.

Article 6. Organització de la seguretat de la informació

1. Els agents de l'organització de la seguretat en la Generalitat exercixen papers principals en el govern, la gestió i l'administració de la seguretat de la informació. La seua missió consistix a definir l'estratègia corporativa en eixa matèria, traçar, dirigir i monitoritzar els plans per a fer-la efectiva, així com assessorar i prestar servicis.

2. La organització estarà composta per:

A) Responsable de la Informació.

B) Comité de Seguretat de la Informació.

C) Responsable dels Fitxers de Dades de Caràcter Personal.

D) Responsable del Servici.

E) Responsable de Seguretat de la Informació.

F) Responsable de Seguretat dels Fitxers de Dades de Caràcter Personal.

G) Responsable del Sistema.

H) Administradors de la Seguretat del Sistema.

I) Administradors de la Seguretat dels Fitxers de Dades de Caràcter Personal.

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, y previa deliberación del Consell, en la reunión del día 24 de agosto de 2012,

DECRETO

CAPÍTULO I
Disposiciones preliminares

Artículo 1. Objeto

El objeto del presente decreto es establecer el reparto de funciones y responsabilidades en materia de seguridad de la información.

Artículo 2. Ámbito de aplicación

La organización de la seguridad regulada en el presente decreto es aplicable a las Consellerias de la Generalitat, así como a sus entidades autónomas dependientes, a las que se refiere el artículo 5.1 del Texto Refundido de la Ley de Hacienda Pública de la Generalitat, exceptuando a la conselleria con competencias en sanidad y a la Agència Valenciana de Salut.

Artículo 3. Principio general de actuación

La seguridad de la información depende de todas las personas que participan en su tratamiento y compromete a todas las que integran la organización. Todo el personal incluido en el ámbito de aplicación del presente decreto, que participe en el tratamiento de información, incluidos empleados, subcontratistas y terceros, se comprometen a dar un uso correcto a todos los activos que requieran para el desarrollo de sus funciones, a respetar las medidas de seguridad que se establezcan y a notificar lo antes posible a los responsables que corresponda de los eventos y puntos débiles de la seguridad de la información que detecte, de manera que puedan emprenderse las acciones oportunas.

Artículo 4. Definiciones

A los efectos previstos en este decreto, las definiciones, palabras, expresiones y términos han de ser entendidos en el sentido indicado en el glosario de términos incluido en el anexo.

CAPÍTULO II
Estructura organizativa

Artículo 5. Estructura

La estructura organizativa de la seguridad de la información agrupa a los agentes cuyas funciones y responsabilidades abarcan toda la Administración de la Generalitat y sus entidades autónomas, exceptuando a la conselleria con competencias en sanidad y a la Agència Valenciana de Salut.

Artículo 6. Organización de la seguridad de la información

1. Los agentes de la organización de la seguridad en la Generalitat desempeñan papeles principales en el gobierno, la gestión y la administración de la seguridad de la información. Su misión consiste en definir la estrategia corporativa en esa materia, trazar, dirigir y monitorizar los planes para hacerla efectiva, así como asesorar y prestar servicios.

2. La organización estará compuesta por:

a) Responsable de la Información.

B) Comité de Seguridad de la Información.

C) Responsable de los Ficheros de Datos de Carácter Personal.

D) Responsable del Servicio.

E) Responsable de Seguridad de la Información.

F) Responsable de Seguridad de los Ficheros de Datos de Carácter Personal.

G) Responsable del Sistema.

H) Administradores de la Seguridad del Sistema.

I) Administradores de la Seguridad de los Ficheros de Datos de Carácter Personal.

CAPÍTOL III
L'organització de la seguretat de la informació

Article 7. Responsable de la Informació

1. El Responsable de la Informació té la responsabilitat última de l'ús que es faça d'una certa informació i, per tant, de la seua protecció. És responsable últim de qualsevol error o negligència que porte a un incident de confidencialitat o integritat, i establix els requisits de seguretat de la informació.

2. Es designa Responsable de la Informació a la Comissió Interdepartamental per a la Modernització Tecnològica, la Qualitat i la Societat del Coneixement en la Comunitat Valenciana.

3. Las funcions principals són les següents:

a) Aprovar els nivells de seguretat requerits per la informació establits en l'esquema nacional de seguretat, informant el Responsable del Servici.

b) Aprovar els principals riscos residuals assumits per l'organització, junt amb el Responsable del Servici.

c) Aprovar el codi tipus per a l'adopció de bones pràctiques en la gestió de la informació de caràcter personal i en la seua protecció.

d) Proposar millores sobre la política i l'organització de la seguretat de la informació de la Generalitat.

Article 8. Comité de Seguretat de la Informació

1. El Comité de Seguretat de la Informació coordina la seguretat de la informació a nivell de l'Administració de la Generalitat. La coordinació de la seguretat té la finalitat de racionalitzar el gasto i d'evitar disfuncions que permeten incidents de seguretat degut a vulnerabilitats en els sistemes d'informació de la Generalitat.

2. El Comité estarà compost per:

a) Presidència: la persona titular de la direcció general competent en matèria de tecnologies de la informació.

b) Vicepresidència: la persona titular de la subdirecció general competent en matèria de seguretat informàtica.

c) Vocals, que podran delegar la seua representació en un funcionari de l'Administració de la Generalitat, amb el rang almenys de direcció de servici:

1r. La persona titular de la subsecretaria de la conselleria competent en matèria de tecnologies de la informació.

2n. La persona titular de la coordinació de l'Advocacia de la Generalitat competent en matèria de tecnologies de la informació.

3r. La persona titular de la subdirecció general competent en matèria d'infraestructures de tecnologies de la informació.

4t. La persona titular de la subdirecció general competent en matèria de sistemes d'informació d'hisenda.

5é. La persona titular de la subdirecció general competent en matèria d'innovació tecnològica educativa.

6é. La persona titular de l'òrgan directiu del Sistema Arxivístic Valencià.

7é. Els responsables de Seguretat dels Fitxers de Dades de Caràcter Personal.

8é. El Responsable de Seguretat dels Fitxers de Dades de Caràcter Personal de la conselleria amb competències en sanitat.

d) Secretaria: amb veu i vot, la persona titular del servici competent en matèria de seguretat informàtica, que executarà les decisions del Comité de Seguretat de la Informació, convocarà les seues reunions i preparará els temes a tractar. En cas d'absència, vacant o malaltia, exercirà les seues funcions el vocal que designe el Comité de Seguretat de la Informació.

3. Las funcions principals són les següents:

a) Atendre els requisits del Consell i dels diferents departaments, en matèria de seguretat de la informació.

b) Informar regularment de l'estat de la seguretat de la informació al Consell.

c) Promoure la millora contínua del sistema de gestió de la seguretat de la informació.

d) Aprovar l'estratègia d'evolució de l'organització pel que fa a seguretat de la informació, elaborada pel Responsable de Seguretat de la Informació.

e) Coordinar els esforços de les diferents àrees en matèria de seguretat de la informació, per a assegurar que els esforços són consistents, alineats amb l'estratègia decidida en la matèria, i evitar duplicitats.

CAPÍTULO III
La organización de la seguridad de la información

Artículo 7. Responsable de la Información

1. El Responsable de la Información tiene la responsabilidad última del uso que se haga de una cierta información y, por tanto, de su protección. Es responsable último de cualquier error o negligencia que lleve a un incidente de confidencialidad o integridad, y establece los requisitos de seguridad de la información.

2. Se designa Responsable de la Información a la Comisión Interdepartamental para la Modernización Tecnológica, la Calidad y la Sociedad del Conocimiento en la Comunitat Valenciana.

3. Las funciones principales son las siguientes:

a) Aprobar los niveles de seguridad requeridos por la información establecidos en el Esquema Nacional de Seguridad, informando al Responsable del Servicio.

b) Aprobar los principales riesgos residuales asumidos por la organización, junto al Responsable del Servicio.

c) Aprobar el código tipo para la adopción de buenas prácticas en la gestión de la información de carácter personal y en su protección.

d) Proponer mejoras sobre la política y la organización de la seguridad de la información de la Generalitat.

Artículo 8. Comité de Seguridad de la Información

1. El Comité de Seguridad de la Información coordina la seguridad de la información a nivel de la Administración de la Generalitat. La coordinación de la seguridad tiene la finalidad de racionalizar el gasto y de evitar disfunciones que permitan incidentes de seguridad debido a vulnerabilidades en los sistemas de información de la Generalitat.

2. El Comité estará compuesto por:

a) Presidencia: la persona titular de la Dirección General competente en materia de tecnologías de la información.

b) Vicepresidencia: la persona titular de la Subdirección General competente en materia de seguridad informática.

c) Vocales, que podrán delegar su representación en un funcionario de la Administración de la Generalitat, con el rango al menos de jefatura de servicio:

1º. La persona titular de la Subsecretaría de la Conselleria competente en materia de tecnologías de la información.

2º. La persona titular de la coordinación de la Abogacía de la Generalitat competente en materia de tecnologías de la información.

3º. La persona titular de la subdirección general competente en materia de infraestructuras de tecnologías de la información.

4º. La persona titular de la subdirección general competente en materia de sistemas de información de hacienda.

5º. La persona titular de la subdirección general competente en materia de innovación tecnológica educativa.

6º. La persona titular del órgano directivo del Sistema Archivístico Valenciano.

7º. Los Responsables de Seguridad de los Ficheros de Datos de Carácter Personal.

8º. El Responsable de Seguridad de los Ficheros de Datos de Carácter Personal de la conselleria con competencias en sanidad.

d) Secretaría: con voz y voto, la persona titular del Servicio competente en materia de seguridad informática, que ejecutará las decisiones del Comité de Seguridad de la Información, convocará sus reuniones y preparará los temas a tratar. En caso de ausencia, vacante o enfermedad, ejercerá sus funciones el vocal que designe el Comité de Seguridad de la Información.

3. Las funciones principales son las siguientes:

a) Atender los requisitos del Consell y de los diferentes departamentos, en materia de seguridad de la información.

b) Informar regularmente del estado de la seguridad de la información al Consell.

c) Promover la mejora continua del sistema de gestión de la seguridad de la información.

d) Aprobar la estrategia de evolución de la organización en lo que respecta a seguridad de la información, elaborada por el Responsable de Seguridad de la Información.

e) Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que los esfuerzos son consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.

f) Elaborar i revisar regularment la Política i Organització de la Seguretat de la Informació perquè siga aprovada pel Consell.

g) Proposar l'aprovació de la normativa de seguretat de la informació.

h) Elaborar i aprovar els requisits de formació i qualificació d'administradors, operadors i usuaris, des del punt de vista de seguretat de la informació.

i) Monitoritzar els principals riscos residuals assumits per l'organització i recomanar possibles actuacions respecte d'estos.

j) Monitoritzar l'exercici dels processos de gestió d'incidents de seguretat i recomanar possibles actuacions respecte d'estos. En particular, vetlar per la coordinació de les diferents àrees de seguretat en la gestió d'incidents de seguretat de la informació.

k) Promoure la realització de les auditories periòdiques que permeten verificar el compliment de les obligacions de l'organisme en matèria de seguretat.

l) Aprovar plans de millora de la seguretat de la informació de l'organització. En particular, vetlarà per la coordinació de diferents plans que puguen realitzar-se en diferents àrees.

m) Prioritzar les actuacions en matèria de seguretat quan els recursos siguen limitats.

n) Vetlar perquè la seguretat de la informació es tinga en compte en tots els projectes de tecnologies de la informació des de la seua especificació inicial fins a la seua posada en operació i posterior manteniment, així com en la preservació de la informació que siga requerida després del cessament en la utilització d'este. En particular, haurà de vetlar per la creació i utilització de servicis horitzontals que reduïsquen duplicitats i recolzen un funcionament homogeni de tots els sistemes de tecnologies de la informació.

o) Resoldre els conflictes de responsabilitat que puguen aparéixer entre els diferents responsables i/o entre diferents àrees de l'organització, i elevar aquells casos en què no tinga prou autoritat per a decidir.

4. El Comité de Seguretat de la Informació ajustarà el seu funcionament a les previsions contingudes en el capítol II de la Llei 30/1992, de 26 de novembre, de Règim Jurídic de les Administracions Públiques i del Procediment Administratiu Comú, relatiu als òrgans col·legiats.

5. El Comité de Seguretat de la Informació es reunirà amb caràcter ordinari almenys una vegada a l'any, i amb caràcter extraordinari quan ho decidisca el seu president.

6. El Comité de Seguretat de la Informació podrà demanar de personal tècnic, propi o extern, la informació pertinent per a la presa de les seues decisions. En cas necessari este personal podrà ser convocat pel Comité de Seguretat de la Informació per a la seua assistència a les reunions, en qualitat d'assessors, amb veu però sense vot.

Article 9. Responsable dels Fitxers de Dades de Caràcter Personal

1. El Responsable dels Fitxers de Dades de Caràcter Personal té la missió de vetlar, dins del seu àmbit de competència, pel compliment de la Llei Orgànica 15/1999, de 13 de desembre, de Protecció de Dades de Caràcter Personal, així com del Reglament de desplegament d'esta aprovat pel Reial Decret 1720/2007, de 21 de desembre.

Haurà d'exercir les seues funcions de forma coordinada amb el Responsable de Seguretat de la Informació.

2. Es designa Responsable dels Fitxers de Dades de Caràcter Personal de cada conselleria o entitat autònoma dependent, a la persona titular de l'òrgan a què corresponguen les funcions establides en l'article 69 de la Llei del Consell en cada conselleria i de l'òrgan de caràcter directiu que tinga atribuïdes les competències sobre els servicis comuns de cada entitat autònoma.

3. Las funcions principals són les següents:

a) Nomenar els administradors de Seguretat dels Fitxers de Dades de Caràcter Personal que considere necessaris per a auxiliar-lo, entre els funcionaris pertanyents a la seua organització, i delegarà les funcions que crega oportunes amb els límits que la normativa li permeta.

b) Adequar les actuacions en esta matèria al codi tipus aprovat per a l'adopció de bones pràctiques en la gestió de la informació de caràcter personal.

f) Elaborar y revisar regularmente la Política y Organización de la Seguridad de la Información para que sea aprobada por el Consell.

g) Proponer la aprobación de la normativa de seguridad de la información.

h) Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios, desde el punto de vista de seguridad de la información.

i) Monitorizar los principales riesgos residuales asumidos por la organización y recomendar posibles actuaciones respecto de ellos.

j) Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto de ellos. En particular, velar por la coordinación de las diferentes áreas de seguridad en la gestión de incidentes de seguridad de la información.

k) Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.

l) Aprobar planes de mejora de la seguridad de la información de la organización. En particular, velará por la coordinación de diferentes planes que puedan realizarse en diferentes áreas.

m) Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.

n) Velar porque la seguridad de la información se tenga en cuenta en todos los proyectos de tecnologías de la información desde su especificación inicial hasta su puesta en operación y posterior mantenimiento, así como en la preservación de la información que sea requerida tras el cese en la utilización del mismo. En particular, deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas de tecnologías de la información.

o) Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas de la organización, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.

4. El Comité de Seguridad de la Información ajustará su funcionamiento a las previsiones contenidas en el capítulo II de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, relativo a los órganos colegiados.

5. El Comité de Seguridad de la Información se reunirá con carácter ordinario al menos una vez al año, y con carácter extraordinario cuando lo decida su Presidente.

6. El Comité de Seguridad de la Información podrá recabar de personal técnico, propio o externo, la información pertinente para la toma de sus decisiones. En caso necesario este personal podrá ser convocado por el Comité de Seguridad de la Información para su asistencia a las reuniones, en calidad de asesores, con voz pero sin voto.

Artículo 9. Responsable de los Ficheros de Datos de Carácter Personal

1. El Responsable de los Ficheros de Datos de Carácter Personal tiene la misión de velar, dentro de su ámbito de competencia, por el cumplimiento de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, así como del Reglamento de desarrollo de la misma aprobado por el Real Decreto 1720/2007, de 21 de diciembre.

Debe ejercer sus funciones de forma coordinada con el Responsable de Seguridad de la Información.

2. Se designa Responsable de los Ficheros de Datos de Carácter Personal de cada Conselleria o entidad autónoma dependiente, a la persona titular del órgano al que correspondan las funciones establecidas en el artículo 69 de la Ley del Consell en cada Conselleria y del órgano de carácter directivo que tenga atribuidas las competencias sobre los servicios comunes de cada entidad autónoma.

3. Las funciones principales son las siguientes:

a) Nombrar a los Administradores de Seguridad de los Ficheros de Datos de Carácter Personal que considere necesarios para auxiliarle, entre los funcionarios pertenecientes a su organización, delegando las funciones que estime oportunas con los límites que la normativa le permita.

b) Adecuar las actuaciones en esta materia al código tipo aprobado para la adopción de buenas prácticas en la gestión de la información de carácter personal.

Article 10. Responsable del Servici

1. El Responsable del Servici té la responsabilitat última de l'ús que es faça de determinats servicis i, per tant, de la seua protecció. És el responsable últim de qualsevol error o negligència que porte a un incident de disponibilitat del servici.

Establix els requisits de seguretat dels servicis, generalment a partir de la informació que tracten i altres requisits derivats del context intern i extern de l'Administració de la Generalitat.

2. Es designa Responsable del Servici la persona titular de l'òrgan a què corresponguen les funcions establides en l'article 73.2 de la Llei del Consell en cada conselleria i de l'òrgan de caràcter directiu que tinga atribuïdes les competències sobre els servicis generals de cada entitat autònoma.

3. Las funcions principals són les següents:

a) Establir els requisits dels servicis en matèria de seguretat, en el marc de l'annex I de l'Esquema Nacional de Seguretat, equival a la potestat de determinar els nivells de seguretat requerits en cada dimensió del servici.

b) Assegurar que la prestació d'un servici sempre haja d'atendre als requisits de seguretat de la informació que maneja, de manera que poden heretar-se els requisits de seguretat d'esta, i afegir requisits de disponibilitat, així com altres com a accessibilitat, interoperabilitat, etc.

Article 11. Responsable de Seguretat de la Informació

1. El Responsable de Seguretat de la Informació té la responsabilitat de vetlar per la seguretat de la informació i dels servicis prestats pels sistemes d'informació, d'acord amb el que establix la política de seguretat de la informació.

És el responsable de la supervisió de l'eficàcia de les mesures de seguretat establides per a protegir la informació i els servicis prestats pels sistemes d'informació.

Assessora a altres responsables en la determinació de les mesures de seguretat necessàries a partir dels requisits de seguretat establits pel context intern i extern de l'organització.

2. Es designa Responsable de Seguretat de la Informació a la persona titular del servici competent en matèria de seguretat informàtica de la direcció general amb competèn-cies en matèria de tecnologies de la informació.

3. Las funcions principals són les següents:

a) Proposar al Responsable de la Informació els nivells de seguretat requerits per la informació, una vegada consultat al responsable del sistema.

b) Proposar al Responsable del Servici els nivells de seguretat requerits pel servici, una vegada consultat al Responsable del Sistema.

c) Promoure la formació i conscienciació en matèria de seguretat de la informació dins del seu àmbit de responsabilitat.

d) Recopilar els requisits de seguretat dels responsables d'Informació i Servici i determinar la categoria del sistema.

e) Realitzar l'anàlisi de riscos.

f) Elaborar una declaració d'aplicabilitat a partir de les mesures de seguretat requerides conforme a l'annex II de l'Esquema Nacional de Seguretat i del resultat de l'anàlisi de riscos.

g) Elaborar i aprovar les directrius per a considerar la seguretat de la informació durant tot el cicle de vida dels actius i processos: especificació, arquitectura, desenrotllament, operació i canvis.

h) Detectar els principals riscos residuals assumits per l'organització, recomanar possibles actuacions respecte d'estos i informar-ne al responsable de sistemes.

i) Elaborar, gestionar i avaluar el codi tipus per a l'adopció de bones pràctiques en la gestió de la informació de caràcter personal i en la seua protecció.

j) Definir mesures i controls establits en la normativa de protecció de dades.

k) Elaborar la memòria anual sobre l'estat de la seguretat de la informació, amb el progrés dels projectes dels plans de millora, resum de les actuacions en matèria de seguretat, dels incidents relatius a seguretat de la informació, de l'estat de la seguretat del sistema, i en particular del nivell de risc residual a què està exposat el sistema.

Artículo 10. Responsable del Servicio

1. El Responsable del Servicio tiene la responsabilidad última del uso que se haga de determinados servicios y, por tanto, de su protección. Es el responsable último de cualquier error o negligencia que lleve a un incidente de disponibilidad del servicio.

Establece los requisitos de seguridad de los servicios, generalmente a partir de la información que tratan y otros requisitos derivados del contexto interno y externo de la Administración de la Generalitat.

2. Se designa Responsable del Servicio a la persona titular del órgano al que correspondan las funciones establecidas en el artículo 73.2 de la Ley del Consell en cada Conselleria y del órgano de carácter directivo que tenga atribuidas las competencias sobre los servicios generales de cada entidad autónoma.

3. Las funciones principales son las siguientes:

a) Establecer los requisitos de los servicios en materia de seguridad, en el marco del anexo I del Esquema Nacional de Seguridad, equivale a la potestad de determinar los niveles de seguridad requeridos en cada dimensión del servicio.

b) Asegurar que la prestación de un servicio siempre deba atender a los requisitos de seguridad de la información que maneja, de forma que pueden heredarse los requisitos de seguridad de la misma, añadiendo requisitos de disponibilidad, así como otros como accesibilidad, interoperabilidad, etc.

Artículo 11. Responsable de Seguridad de la Información

1. El Responsable de Seguridad de la Información tiene la responsabilidad de velar por la seguridad de la información y de los servicios prestados por los sistemas de información, de acuerdo a lo establecido en la Política de Seguridad de la Información.

Es el responsable de la supervisión de la eficacia de las medidas de seguridad establecidas para proteger la información y los servicios prestados por los sistemas de información.

Asesora a otros responsables en la determinación de las medidas de seguridad necesarias a partir de los requisitos de seguridad establecidos por el contexto interno y externo de la organización.

2. Se designa Responsable de Seguridad de la Información a la persona titular del Servicio competente en materia de seguridad informática de la Dirección General con competencias en materia de tecnologías de la información.

3. Las funciones principales son las siguientes:

a) Proponer al Responsable de la Información los niveles de seguridad requeridos por la información, una vez consultado al Responsable del Sistema.

b) Proponer al Responsable del Servicio los niveles de seguridad requeridos por el servicio, una vez consultado al Responsable del Sistema.

c) Promover la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad.

d) Recopilar los requisitos de seguridad de los Responsables de Información y Servicio y determinar la categoría del sistema.

e) Realizar el análisis de riesgos.

f) Elaborar una declaración de aplicabilidad a partir de las medidas de seguridad requeridas conforme al anexo II del Esquema Nacional de Seguridad y del resultado del análisis de riesgos.

g) Elaborar y aprobar las directrices para considerar la seguridad de la información durante todo el ciclo de vida de los activos y procesos: especificación, arquitectura, desarrollo, operación y cambios.

h) Detectar los principales riesgos residuales asumidos por la organización, recomendar posibles actuaciones respecto de ellos e informar de los mismos al Responsable de Sistemas.

i) Elaborar, gestionar y evaluar el código tipo para la adopción de buenas prácticas en la gestión de la información de carácter personal y en su protección.

j) Definir medidas y controles establecidos en la normativa de protección de datos.

k) Elaborar la memoria anual sobre el estado de la seguridad de la información, con el progreso de los proyectos de los planes de mejora, resumen de las actuaciones en materia de seguridad, de los incidentes relativos a seguridad de la información, del estado de la seguridad del sistema, y en particular del nivel de riesgo residual al que está expuesto el sistema.

l) Elaborar la revisió de la política i organització de la seguretat de la informació.

m) Elaborar i revisar la normativa de seguretat de la informació.

n) Elaborar i aprovar els procediments operatius de seguretat de la informació.

o) Elaborar i aprovar guies de bones pràctiques de seguretat de la informació.

p) Elaborar, junt amb el Responsable del Sistema, plans de millora de la seguretat, per a la seua aprovació pel Comité de Seguretat de la Informació.

q) Validar els plans de continuïtat de sistemes.

r) Elaborar els plans de formació i conscienciació del personal en seguretat de la informació, que hauran de ser aprovats pel Comité de Seguretat de la Informació.

s) Ser responsable en cas que ocórreguen incidents de seguretat de la informació.

t) Analitzar i proposar salvaguardes que previnguen incidents semblants en un futur.

u) Vetlar per la seguretat i continuïtat de les instal·lacions, xarxes, sistemes i equips físics i de tecnologia de la informació sobre les quals descansa el funcionament dels servicis essencials.

4. A través del Centre de Seguretat en Tecnologies de la Informació de la Comunitat Valenciana, realitzarà les funcions següents:

a) La gestió d'incidents de seguretat de la informació a nivell corporatiu.

b) Coordinar amb el Centre de Capacitat de Resposta davant d'Incidents de Seguretat de la Informació, del Centre Criptològic Nacional, els incidents que puguen ocórrer dins de l'àmbit de l'administració pública.

c) Establir relacions amb altres centres semblants, tant a nivell nacional com internacional, que permeten actuar en casos d'amenaces o incidents externs.

d) Monitoritzar la presència d'informació de la Generalitat en Internet, verificant que no supose un risc.

e) Monitoritzar la xarxa corporativa per a detectar amenaces de seguretat per als seus actius.

f) Realitzar auditories tècniques sobre els recursos més exposats i auditories normatives que permeten complir amb la legislació vigent.

g) Ser un centre d'alerta primerenca que notifique al responsable corresponent dels incidents o amenaces que requerisquen de la seua atenció, i facilitar la informació detallada que permeta resoldre el problema.

h) Fomentar l'ús de servicis preventius de seguretat que permeten mitigar els incidents futurs o reduir el seu impacte.

5. Delegació de funcions:

a) En determinats sistemes d'informació que, per la seua complexitat, distribució, separació física dels seus elements o números d'usuaris, es necessite de personal addicional per a dur a terme les funcions del Responsable de Seguretat de la Informació, es podran designar quants responsables de Seguretat de la Informació Delegats es consideren necessaris.

b) Es designarà com a responsables de Seguretat de la Informació delegats a funcionaris, que seran nomenats, per resolució administrativa, a proposta del Responsable de Seguretat de la Informació. La responsabilitat final continua recaient sobre el Responsable de Seguretat de la Informació.

c) Els delegats es faran càrrec, en el seu àmbit, de totes aquelles funcions que li siguen delegades pel Responsable de la Seguretat de la Informació. Cada delegat tindrà una dependència funcional directa del Responsable de la Seguretat de la Informació, que és a qui informa.

Article 12. Responsable de Seguretat dels Fitxers de Dades de Caràcter Personal

1. El Responsable de Seguretat dels Fitxers de Dades de Caràcter Personal té la missió, dins del seu àmbit de competència, de coordinar i controlar les mesures de seguretat aplicables sobre els fitxers de dades de caràcter personal.

2. Se designa Responsable de Seguretat dels Fitxers de Dades de Caràcter Personal de cada conselleria o entitat autònoma dependent, a la persona titular de l'òrgan a què corresponguen les funcions establides en l'article 73.2 de la Llei del Consell en cada conselleria i de l'òrgan de

l) Elaborar la revisión de la política y organización de la seguridad de la información.

m) Elaborar y revisar la normativa de seguridad de la información.

n) Elaborar y aprobar los procedimientos operativos de seguridad de la información.

o) Elaborar y aprobar guías de buenas prácticas de seguridad de la información.

p) Elaborar, junto al Responsable del Sistema, planes de mejora de la seguridad, para su aprobación por el Comité de Seguridad de la Información.

q) Validar los planes de continuidad de sistemas.

r) Elaborar los planes de formación y concienciación del personal en seguridad de la información, que deberán ser aprobados por el Comité de Seguridad de la Información.

s) Ser responsable en caso de ocurrencia de incidentes de seguridad de la información.

t) Analizar y proponer salvaguardas que prevengan incidentes similares en un futuro.

u) Velar por la seguridad y continuidad de las instalaciones, redes, sistemas y equipos físicos y de tecnología de la información sobre las que descansa el funcionamiento de los servicios esenciales.

4. A través del Centro de Seguridad en Tecnologías de la Información de la Comunitat Valenciana, realizará las siguientes funciones:

a) La gestión de incidentes de seguridad de la información a nivel corporativo.

b) Coordinar con el Centro de Capacidad de Respuesta ante Incidentes de Seguridad de la Información, del Centro Criptológico Nacional, los incidentes que puedan ocurrir dentro del ámbito de la administración pública.

c) Establecer relaciones con otros centros similares, tanto a nivel nacional como internacional, que permitan actuar en casos de amenazas o incidentes externos.

d) Monitorizar la presencia de información de la Generalitat en Internet, verificando que no suponga un riesgo.

e) Monitorizar la red corporativa para detectar amenazas de seguridad para sus activos.

f) Realizar auditorías técnicas sobre los recursos más expuestos y auditorías normativas que permitan cumplir con la legislación vigente.

g) Ser un centro de alerta temprana que notifique al responsable correspondiente de los incidentes o amenazas que requieran de su atención, facilitando la información detallada que permita resolver el problema.

h) Fomentar el uso de servicios preventivos de seguridad que permitan mitigar los incidentes futuros o reducir su impacto.

5. Delegación de funciones:

a) En determinados sistemas de información que, por su complejidad, distribución, separación física de sus elementos o números de usuarios, se necesite de personal adicional para llevar a cabo las funciones del Responsable de Seguridad de la Información, se podrán designar cuantos Responsables de Seguridad de la Información Delegados se consideren necesarios.

b) Se designará como responsables de Seguridad de la Información delegados a funcionarios, que serán nombrados, por resolución administrativa, a propuesta del Responsable de Seguridad de la Información. La responsabilidad final sigue recayendo sobre el Responsable de Seguridad de la Información.

c) Los delegados se harán cargo, en su ámbito, de todas aquellas funciones que le sean delegadas por el Responsable de la Seguridad de la Información. Cada delegado tendrá una dependencia funcional directa del Responsable de la Seguridad de la Información, que es a quien informa.

Artículo 12. Responsable de Seguridad de los Ficheros de Datos de Carácter Personal

1. El Responsable de Seguridad de los Ficheros de Datos de Carácter Personal tiene la misión, dentro de su ámbito de competencia, de coordinar y controlar las medidas de seguridad aplicables sobre los ficheros de datos de carácter personal.

2. Se designa Responsable de Seguridad de los Ficheros de Datos de Carácter Personal de cada Conselleria o entidad autónoma dependiente, a la persona titular del órgano al que correspondan las funciones establecidas en el artículo 73.2 de la Ley del Consell en cada Conselleria y

caràcter directiu que tinga atribuïdes les competències sobre els servicis generals de cada entitat autònoma.

3. Les funcions principals són les següents:

a) Coordinar i controlar les mesures de seguretat definides en el document de seguretat, aplicables als fitxers automatitzats i no automatitzats, detallades en els articles 89 al 114 del Reial Decret 1720/2007, de 21 de desembre, pel qual s'aprova el Reglament de Desplegament de la LOPD.

b) Informar al Responsable dels Fitxers de Dades de Caràcter Personal d'aquells fets rellevants relacionats amb les mesures de seguretat definides en el document de seguretat, amb la periodicitat i en resposta als esdeveniments que s'establisquen.

Article 13. Responsable del Sistema

1. El Responsable del Sistema té la missió de desenrotllar, operar i mantindre el sistema d'informació durant tot el seu cicle de vida, de les seues especificacions, instal·lacions i verificació del seu funcionament correcte.

2. Es designa Responsable del Sistema a la persona titular de la subdirecció general competent en matèria d'infraestructures de tecnologies de la informació.

3. Les funcions principals són les següents:

a) Definir i mantindre la infraestructura i sistema de gestió del sistema d'informació establint els criteris d'ús i els servicis disponibles en este.

b) Implantar les mesures per a garantir la seguretat informàtica dels sistemes d'informació.

c) Acordar la suspensió del maneig d'una certa informació o la prestació d'un cert servici, si és informat de deficiències greus de seguretat que pogueren afectar la satisfacció dels requisits establits.

d) Aplicar els procediments operatius de seguretat elaborats i aprovats pel Responsable de Seguretat.

e) Monitoritzar l'estat de la seguretat dels sistemes d'informació, i informar periòdicament, davant d'incidents de seguretat rellevants, al Responsable de Seguretat de la Informació.

f) Elaborar els plans de continuïtat del sistema, que seran aprovats pel Comité de Seguretat de la Informació.

g) Realitzar exercicis i proves periòdiques dels plans de continuïtat del sistema per a mantindre actualitzats i verificar que són efectius.

h) En el cas que ocórreguen incidents de seguretat de la informació:

1r. Planificar la implantació de les salvaguardes en el sistema.

2n. Executar el pla de seguretat aprovat.

i) Nomenar els administradors de la Seguretat del Sistema.

j) Implantar les mesures de seguretat definides en el document de seguretat, aplicables als fitxers automatitzats, detallades en els articles 93 al 104 del Reial Decret 1720/2007, de 21 de desembre, pel qual s'aprova el Reglament de Desplegament de la LOPD.

4. Delegació de funcions:

a) En determinats sistemes d'informació que, per la seua complexitat, distribució, separació física dels seus elements o números d'usuaris, es necessite de personal addicional per a dur a terme les funcions del Responsable del Sistema podrà designar quants responsables del Sistema delegats considere necessaris.

b) Es designarà com a responsables del Sistema delegats a funcionaris, que seran nomenats, per resolució administrativa, a proposta del Responsable del Sistema. La responsabilitat final continua recaient sobre el Responsable del Sistema.

c) Els delegats es faran càrrec, en el seu àmbit, de totes aquelles funcions que delegue el Responsable del Sistema.

d) Cada delegat tindrà una dependència funcional directa del Responsable del Sistema, que és a qui informa.

Article 14. Administradors de la Seguretat del Sistema

1. Els administradors de la Seguretat del Sistema tenen la missió de la implementació, gestió i manteniment de les mesures de seguretat aplicables en el sistema d'informació.

2. Es designarà com a administradors de la Seguretat del Sistema a funcionaris que seran nomenats, per resolució administrativa, a proposta del Responsable del Sistema.

del órgano de carácter directivo que tenga atribuidas las competencias sobre los servicios generales de cada entidad autónoma.

3. Las funciones principales son las siguientes:

a) Coordinar y controlar las medidas de seguridad definidas en el documento de seguridad, aplicables a los ficheros automatizados y no automatizados, detalladas en los artículos 89 al 114 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD.

b) Informar al Responsable de los Ficheros de Datos de Carácter Personal de aquellos hechos relevantes relacionados con las medidas de seguridad definidas en el documento de seguridad, con la periodicidad y en respuesta a los eventos que se establezcan.

Artículo 13. Responsable del Sistema

1. El Responsable del Sistema tiene la misión de desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, de sus especificaciones, instalaciones y verificación de su correcto funcionamiento.

2. Se designa Responsable del Sistema a la persona titular de la Subdirección General competente en materia de infraestructuras de tecnologías de la información.

3. Las funciones principales son las siguientes:

a) Definir y mantener la infraestructura y sistema de gestión del sistema de información, estableciendo los criterios de uso y los servicios disponibles en el mismo.

b) Implantar las medidas para garantizar la seguridad informática de los sistemas de información.

c) Acordar la suspensión del manejo de una cierta información o la prestación de un cierto servicio, si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos.

d) Aplicar los procedimientos operativos de seguridad elaborados y aprobados por el Responsable de Seguridad.

e) Monitorizar el estado de la seguridad de los sistemas de información, e informar periódicamente, ante incidentes de seguridad relevantes, al Responsable de Seguridad de la Información.

f) Elaborar los planes de continuidad del sistema, que serán aprobados por el Comité de Seguridad de la Información.

g) Realizar ejercicios y pruebas periódicas de los planes de continuidad del sistema para mantenerlos actualizados y verificar que son efectivos.

h) En el caso de ocurrir incidentes de seguridad de la información:

1º. Planificar la implantación de las salvaguardas en el sistema.

2º. Ejecutar el plan de seguridad aprobado.

i) Nombrar a los Administradores de la Seguridad del Sistema.

j) Implantar las medidas de seguridad definidas en el Documento de Seguridad, aplicables a los ficheros automatizados, detalladas en los artículos 93 al 104 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD.

4. Delegación de funciones:

a) En determinados sistemas de información que, por su complejidad, distribución, separación física de sus elementos o números de usuarios, se necesite de personal adicional para llevar a cabo las funciones del Responsable del Sistema podrá designar cuantos Responsables del Sistema Delegados considere necesarios.

b) Se designará como Responsables del Sistema Delegados a funcionarios, que serán nombrados, por resolución administrativa, a propuesta del Responsable del Sistema. La responsabilidad final sigue recayendo sobre el Responsable del Sistema.

c) Los delegados se harán cargo, en su ámbito, de todas aquellas funciones que delegue el Responsable del Sistema.

d) Cada delegado tendrá una dependencia funcional directa del Responsable del Sistema, que es a quien informa.

Artículo 14. Administradores de la Seguridad del Sistema

1. Los Administradores de la Seguridad del Sistema tienen la misión de la implementación, gestión y mantenimiento de las medidas de seguridad aplicables en el sistema de información.

2. Se designará como Administradores de la Seguridad del Sistema a funcionarios que serán nombrados, por resolución administrativa, a propuesta del Responsable del Sistema.

3. Las funcions principals són les següents:

a) Implementar, gestionar i mantindre les mesures de seguretat aplicables al sistema d'informació.

b) Assegurar que els controls de seguretat establits es complixen estrictament.

c) Aplicar als sistemes, usuaris i altres actius i recursos relacionats amb este, tant interns com externs, els procediments operatius de seguretat i els mecanismes i servicis de seguretat requerits.

d) Assegurar que són aplicats els procediments aprovats per a manejar els sistemes d'informació i els mecanismes i servicis de seguretat requerits.

e) Aprovar els canvis en la configuració vigent del sistema d'informació, i garantir que seguisquen operatius els mecanismes i servicis de seguretat habilitats.

f) Informar als responsables de la Seguretat i del Sistema de qualsevol anomalia, compromís o vulnerabilitat relacionada amb la seguretat.

g) Monitoritzar l'estat de la seguretat del sistema.

3.1. Quant a la gestió de projectes informàtics:

a) Implementar les directrius per a considerar la seguretat de la informació durant tot el cicle de vida dels actius i processos: especificació, arquitectura, desenrotllament, operació i canvis.

b) En relació amb el desenrotllament d'aplicacions, assegurar que la traçabilitat, pistes d'auditoria i altres registres de seguretat requerits es troben habilitats i registren amb la freqüència desitjada, d'acord amb la política de seguretat establida per l'organització.

3.2. Quant als llocs de treball:

a) Gestionar, configurar i actualitzar els equips i les aplicacions en què es basen els mecanismes i servicis de seguretat del sistema d'informació.

b) Supervisar les instal·lacions dels equips i les aplicacions, les seues modificacions i millores per a assegurar que la seguretat no està compromesa.

3.3. En el cas que ocórreguen incidents de seguretat de la informació:

a) Dur a terme el registre, comptabilitat i gestió dels incidents de seguretat en els sistemes sota la seua responsabilitat.

b) Executar el pla de seguretat aprovat.

c) Aïllar l'incident per a evitar la propagació a elements aliens a la situació de risc.

d) Prendre decisions a curt termini si la informació s'ha vist compromesa de tal forma que poguera tindre conseqüències greus.

e) Assegurar la integritat dels elements crítics del sistema si s'ha vist afectada la disponibilitat d'estos.

f) Mantindre i recuperar la informació emmagatzemada pel sistema i els seus servicis associats.

g) Investigar l'incident: determinar el mode, els mitjans, els motius i l'origen de l'incident.

Article 15. Administradors de la Seguretat dels Fitxers de Dades de Caràcter Personal

1. Els administradors de la Seguretat dels Fitxers de Dades de Caràcter Personal tenen com a missió l'execució d'una sèrie de tasques que, sent responsabilitat del Responsable dels Fitxers de Dades de Caràcter Personal, les tenen delegades i així consten en el corresponent document de seguretat de protecció de dades.

2. Es designarà com a administradors de la Seguretat dels Fitxers de Dades de Caràcter Personal a funcionaris, que seran nomenats, per resolució administrativa, pel Responsable dels Fitxers de Dades de Caràcter Personal corresponent.

3. Las funcions principals, són les següents:

a) Mantindre el document de seguretat en tot moment actualitzat i adequat a les disposicions vigents.

b) Exercir les funcions de control o autoritzacions.

c) Gestionar l'exercici dels drets d'accés, rectificació, cancel·lació i oposició.

d) Tramitar la publicació en el *Diari Oficial de la Comunitat Valenciana* de l'oportuna disposició de creació del fitxer. Així com la notificació dels fitxers de dades personals que es creen al Registre General de Protecció de Dades de l'Agència Espanyola de Protecció de Dades,

3. Las funciones principales son las siguientes:

a) Implementar, gestionar y mantener las medidas de seguridad aplicables al sistema de información.

b) Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.

c) Aplicar a los sistemas, usuarios y otros activos y recursos relacionados con el mismo, tanto internos como externos, los procedimientos operativos de seguridad y los mecanismos y servicios de seguridad requeridos.

d) Asegurar que son aplicados los procedimientos aprobados para manejar los sistemas de información y los mecanismos y servicios de seguridad requeridos.

e) Aprobar los cambios en la configuración vigente del sistema de información, garantizando que sigan operativos los mecanismos y servicios de seguridad habilitados.

f) Informar a los responsables de la Seguridad y del Sistema de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.

g) Monitorizar el estado de la seguridad del sistema.

3.1. En cuanto a la gestión de proyectos informáticos:

a) Implementar las directrices para considerar la seguridad de la información durante todo el ciclo de vida de los activos y procesos: especificación, arquitectura, desarrollo, operación y cambios.

b) En relación con el desarrollo de aplicaciones, asegurar que la trazabilidad, pistas de auditoría y otros registros de seguridad requeridos se encuentren habilitados y registren con la frecuencia deseada, de acuerdo con la política de seguridad establecida por la organización.

3.2. En cuanto a los puestos de trabajo:

a) Gestionar, configurar y actualizar los equipos y las aplicaciones en los que se basan los mecanismos y servicios de seguridad del sistema de información.

b) Supervisar las instalaciones de los equipos y las aplicaciones, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida.

3.3. En el caso de ocurrir incidentes de seguridad de la información:

a) Llevar a cabo el registro, contabilidad y gestión de los incidentes de seguridad en los sistemas bajo su responsabilidad.

b) Ejecutar el plan de seguridad aprobado.

c) Aislar el incidente para evitar la propagación a elementos ajenos a la situación de riesgo.

d) Tomar decisiones a corto plazo si la información se ha visto comprometida de tal forma que pudiera tener consecuencias graves.

e) Asegurar la integridad de los elementos críticos del sistema si se ha visto afectada la disponibilidad de los mismos.

f) Mantener y recuperar la información almacenada por el sistema y sus servicios asociados.

g) Investigar el incidente: determinar el modo, los medios, los motivos y el origen del incidente.

Artículo 15. Administradores de la Seguridad de los Ficheros de Datos de Carácter Personal

1. Los Administradores de la Seguridad de los Ficheros de Datos de Carácter Personal tienen como misión la ejecución de una serie de tareas que, siendo responsabilidad del Responsable de los Ficheros de Datos de Carácter Personal, las tienen delegadas y así constan en el correspondiente documento de seguridad de protección de datos.

2. Se designará como Administradores de la Seguridad de los Ficheros de Datos de Carácter Personal a funcionarios, que serán nombrados, por resolución administrativa, por el Responsable de los Ficheros de Datos de Carácter Personal correspondiente.

3. Las funciones principales son las siguientes:

a) Mantener el documento de seguridad en todo momento actualizado y adecuado a las disposiciones vigentes.

b) Ejercer las funciones de control o autorizaciones.

c) Gestionar el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

d) Tramitar la publicación en el *Diari Oficial de la Comunitat Valenciana* de la oportuna disposición de creación del fichero. Así como la notificación de los ficheros de datos personales que se creen al Registro General Protección de Datos de la Agencia Española de Protección de

i de la mateixa manera les seues modificacions rellevants o la seua eliminació.

e) Coordinar l'execució dels procediments d'actuació definits per a garantir el nivell de seguretat exigit.

f) Gestionar el registre d'incidències.

g) Gestionar la relació actualitzada d'usuaris i perfils d'usuaris, i els accessos autoritzats per a cada un d'estos.

h) Gestionar el registre d'entrada i eixida de suports i documents, i de les seues autoritzacions.

i) Implantar les mesures de seguretat definides en el document de seguretat, aplicables als fitxers no automatitzats, detallades en els articles 105 al 114 del Reial Decret 1720/2007, de 21 de desembre, pel qual s'aprova el Reglament de Desplegament de la LOPD.

j) Qualsevol una altra obligació que li delegue el Responsable dels Fitxers de Dades de Caràcter Personal.

DISPOSICIÓ DEROGATÒRIA

Única. Derogació normativa

Queda derogat expressament el capítol III del títol I (articles 10 al 13), així com totes les referències al Registre de Fitxers Informatitzats, del 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. Així mateix queden derogades totes aquelles disposicions del mateix rang o d'un rang inferior que s'oposen o contradiguen al que disposa este decret.

DISPOSICIONS FINALS

Primera. Nomenaments

S'habilita l'òrgan directiu amb competència en tecnologies de la informació per als nomenaments previstos en este decret, excepte el nomenament dels administradors de la Seguretat dels Fitxers de Dades de Caràcter Personal.

Segona. Entrada en vigor

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

Morella, 24 d'agost de 2012

El president de la Generalitat,
ALBERTO FABRA PART

El conseller d'Hisenda i Administració Pública,
JOSÉ MANUEL VELA BARGUES

ANNEX

Glossari de termes

ACTIU: component o funcionalitat d'un sistema d'informació susceptible de ser atacat deliberada o accidentalment amb conseqüències per a l'organització. Inclou: informació, dades, servicis, aplicacions, equips, comunicacions, recursos administratius, recursos físics i recursos humans.

ANÀLISI DE RISCOS: utilització sistemàtica de la informació disponible per a identificar perills i estimar els riscos.

AUDITORIA DE LA SEGURETAT: revisió i examen independents dels registres i activitats del sistema per a verificar la idoneïtat dels controls del sistema, assegurar que es complixen la política de seguretat i els procediments operatius establits, detectar les infraccions de la seguretat i recomanar modificacions apropiades dels controls, de la política i dels procediments.

Datos, y de igual manera sus modificaciones relevantes o su eliminación.

e) Coordinar la ejecución de los procedimientos de actuación definidos para garantizar el nivel de seguridad exigido.

f) Gestionar el registro de incidencias.

g) Gestionar la relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos.

h) Gestionar el registro de entrada y salida de soportes y documentos, y de sus autorizaciones.

i) Implantar las medidas de seguridad definidas en el Documento de Seguridad, aplicables a los ficheros no automatizados, detalladas en los artículos 105 al 114 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD.

j) Cualquier otra obligación que le delegue el Responsable de los Ficheros de Datos de Carácter Personal.

DISPOSICIÓN DEROGATORIA

Única. Derogación normativa

Queda derogado expresamente el capítulo III del título I (artículos 10 al 13), así como todas las referencias al Registro de Ficheros Informatizados, del 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. Asimismo quedan derogadas todas aquellas disposiciones de igual o inferior rango que se opongan o contradigan a lo dispuesto en el presente decreto.

DISPOSICIONES FINALES

Primera. Nombramientos

Se habilita al órgano directivo con competencia en tecnologías de la información para los nombramientos previstos en este decreto, excepto el nombramiento de los Administradores de la Seguridad de los Ficheros de Datos de Carácter Personal.

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*.

Morella, 24 de agosto de 2012

El president de la Generalitat,
ALBERTO FABRA PART

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

ANEXO

Glosario de términos

ACTIVO: componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones, equipos, comunicaciones, recursos administrativos, recursos físicos y recursos humanos.

ANÁLISIS DE RIESGOS: utilización sistemática de la información disponible para identificar peligros y estimar los riesgos.

AUDITORÍA DE LA SEGURIDAD: revisión y examen independientes de los registros y actividades del sistema para verificar la idoneidad de los controles del sistema, asegurar que se cumplen la política de seguridad y los procedimientos operativos establecidos, detectar las infracciones de la seguridad y recomendar modificaciones apropiadas de los controles, de la política y de los procedimientos.

CATEGORIA D'UN SISTEMA: és un nivell, dins de l'escala bàsica-mitjana-alta, amb el qual s'adjectiva un sistema a fi de seleccionar les mesures de seguretat necessàries per a este. La categoria del sistema recull la visió holística del conjunt d'actius com un tot harmònic, orientat a la prestació d'uns servicis.

CODI TIPUS: codi de bona pràctica professional en tractament de dades de caràcter personal, on s'establixen les condicions d'organització, règim de funcionament, procediments aplicables, normes de seguretat de l'entorn, programes o equips, obligacions dels implicats en el tractament, així com les garanties, en el seu àmbit, per a l'exercici dels drets.

CONFIDENCIALITAT: propietat o característica consistent en què la informació ni es posa a disposició, ni es revela a individus, entitats o processos no autoritzats.

DADES DE CARÀCTER PERSONAL: qualsevol informació numèrica, alfabètica, gràfica, fotogràfica, acústica o de qualsevol altre tipus concernent a persones físiques identificades o identificables.

DISPONIBILITAT: propietat o característica dels actius consistent en què les entitats o processos autoritzats tenen accés a estos quan ho requerixen.

ENCARREGAT DEL TRACTAMENT: la persona física o jurídica, pública o privada, o òrgan administratiu que, només o conjuntament amb altres, tracte dades personals per compte del responsable del tractament o del responsable del fitxer, com a conseqüència de l'existència d'una relació jurídica que el vincula amb este i delimita l'àmbit de la seua actuació per a la prestació d'un servici. Podran ser també encarregats del tractament els ens sense personalitat jurídica que actuen en el tràfic com a subjectes diferenciats.

FITXER NO AUTOMATITZAT: tot conjunt de dades de caràcter personal organitzat de forma no automatitzada i estructurat d'acord amb criteris específics relatius a persones físiques, que permeten accedir sense esforços desproporcionats a les seues dades personals, ja siga aquell centralitzat, descentralitzat o repartit de forma funcional o geogràfica.

GESTIÓ D'INCIDENTS: pla d'acció per a atendre les incidències que ocórreguen. A més de resoldre-les, ha d'incorporar mesures d'exercici que permeten conéixer la qualitat del sistema de protecció i detectar tendències abans que es convertisquen en grans problemes.

INCIDÈNCIA: qualsevol anomalia que afecte o poguera afectar la seguretat de les dades.

INTEGRITAT: propietat o característica consistent en què l'actiu d'informació no ha sigut alterat de manera no autoritzada.

MESURES DE SEGURETAT: conjunt de disposicions encaminades a protegir-se dels riscos possibles sobre el sistema d'informació, a fi d'assegurar els seus objectius de seguretat. Pot tractar-se de mesures de prevenció, de dissuasió, de protecció, de detecció i reacció, o de recuperació.

POLÍTICA DE SEGURETAT: conjunt de directrius plasmades en document escrit, que regixen la forma en què una organització gestiona i protegix la informació i els servicis que considera crítics.

RESPONSABLE DE SEGURETAT: en l'àmbit de la protecció de dades de caràcter personal, persona o persones a qui el responsable del fitxer ha assignat formalment la funció de coordinar i controlar les mesures de seguretat aplicables.

RESPONSABLE DEL FITXER O DEL TRACTAMENT: persona física o jurídica, de naturalesa pública o privada, o òrgan administratiu, que sol o conjuntament amb altres decidisca sobre la finalitat, contingut i ús del tractament, encara que no ho realitzara materialment. Podran ser també responsables del fitxer o del tractament els ens sense personalitat jurídica que actuen en el tràfic com a subjectes diferenciats.

CATEGORÍA DE UN SISTEMA: es un nivel, dentro de la escala Básica-Media-Alta, con el que se adjetiva un sistema a fin de seleccionar las medidas de seguridad necesarias para el mismo. La categoría del sistema recoge la visión holística del conjunto de activos como un todo armónico, orientado a la prestación de unos servicios.

CÓDIGO TIPO: código de buena práctica profesional en tratamiento de datos de carácter personal, donde se establecen las condiciones de organización, régimen de funcionamiento, procedimientos aplicables, normas de seguridad del entorno, programas o equipos, obligaciones de los implicados en el tratamiento, así como las garantías, en su ámbito, para el ejercicio de los derechos.

CONFIDENCIALIDAD: propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.

DATOS DE CARÁCTER PERSONAL: cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables.

DISPONIBILIDAD: propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.

ENCARGADO DEL TRATAMIENTO: la persona física o jurídica, pública o privada, u órgano administrativo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento o del responsable del fichero, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio. Podrán ser también encargados del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

FICHERO NO AUTOMATIZADO: todo conjunto de datos de carácter personal organizado de forma no automatizada y estructurado conforme a criterios específicos relativos a personas físicas, que permitan acceder sin esfuerzos desproporcionados a sus datos personales, ya sea aquél centralizado, descentralizado o repartido de forma funcional o geográfica.

GESTIÓN DE INCIDENTES: plan de acción para atender a las incidencias que ocurran. Además de resolverlas debe incorporar medidas de desempeño que permitan conocer la calidad del sistema de protección y detectar tendencias antes de que se conviertan en grandes problemas.

INCIDENCIA: cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos.

INTEGRIDAD: Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.

MEDIDAS DE SEGURIDAD: conjunto de disposiciones encaminadas a protegerse de los riesgos posibles sobre el sistema de información, con el fin de asegurar sus objetivos de seguridad. Puede tratarse de medidas de prevención, de disuasión, de protección, de detección y reacción, o de recuperación.

POLÍTICA DE SEGURIDAD: conjunto de directrices plasmadas en documento escrito, que rigen la forma en que una organización gestiona y protege la información y los servicios que considera críticos.

RESPONSABLE DE SEGURIDAD: en el ámbito de la protección de datos de carácter personal, persona o personas a las que el responsable del fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables.

RESPONSABLE DEL FICHERO O DEL TRATAMIENTO: persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que solo o conjuntamente con otros decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente. Podrán ser también responsables del fichero o del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

RISC: estimació del grau d'exposició a què una amenaça es materialitze sobre un o més actius causant danys o perjuís a l'organització.

SISTEMA DE GESTIÓ DE LA SEGURETAT DE LA INFORMACIÓ (SGSI): sistema de gestió que, basat en l'estudi dels riscos, s'estableix per a crear, implementar, fer funcionar, supervisar, revisar, mantindre i millorar la seguretat de la informació. El sistema de gestió inclou l'estructura organitzativa, les polítiques, les activitats de planificació, les responsabilitats, les pràctiques, els procediments, els processos i els recursos.

SISTEMA D'INFORMACIÓ: conjunt organitzat de recursos perquè la informació es puga recollir, emmagatzemar, processar o tractar, mantindre, usar, compartir, distribuir, posar a disposició, presentar o transmetre.

TRAÇABILITAT: propietat o característica consistent en què les actuacions d'una entitat poden ser imputades exclusivament a esta entitat.

VULNERABILITAT: una debilitat que pot ser aprofitada per una amenaça.

RIESGO: estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización.

SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI): sistema de gestión que, basado en el estudio de los riesgos, se establece para crear, implementar, hacer funcionar, supervisar, revisar, mantener y mejorar la seguridad de la información. El sistema de gestión incluye la estructura organizativa, las políticas, las actividades de planificación, las responsabilidades, las prácticas, los procedimientos, los procesos y los recursos.

SISTEMA DE INFORMACIÓN: conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir.

TRAZABILIDAD: propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.

VULNERABILIDAD: una debilidad que puede ser aprovechada por una amenaza.