I. DISPOSICIONS GENERALS

MINISTERI DE LA PRESIDÈNCIA

11881 *Reial decret 951/2015, de 23 d'octubre, de modificació del Reial decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat en l'àmbit de l'Administració electrònica.*

La Llei 11/2007, de 22 de juny, d'accés electrònic dels ciutadans als serveis públics, va establir l'Esquema Nacional de Seguretat que, aprovat mitjançant el Reial decret 3/2010, de 8 de gener, té per objecte determinar la política de seguretat en la utilització de mitjans electrònics en el seu àmbit d'aplicació i està constituït pels principis bàsics i els requisits mínims que permetin una protecció adequada de la informació. També va establir que aquest Esquema s'havia de mantenir actualitzat de manera permanent i, en desplegament d'aquest precepte, el Reial decret 3/2010, de 8 de gener, estableix que l'Esquema Nacional de Seguretat s'ha de desenvolupar i perfeccionar al llarg del temps en paral·lel al progrés dels serveis d'administració electrònica, l'evolució de la tecnologia, els nous estàndards internacionals sobre seguretat i auditoria, i la consolidació de les infraestructures que li serveixen de suport, i s'ha de mantenir actualitzat de manera permanent.

Posteriorment, la Llei 40/2015, d'1 d'octubre, de règim jurídic del sector públic, estableix que les administracions públiques s'han de relacionar entre si i amb els seus òrgans, organismes públics i entitats vinculats o dependents a través de mitjans electrònics, que assegurin la interoperabilitat i seguretat dels sistemes i les solucions adoptades per cadascuna d'aquestes, han de garantir la protecció de les dades de caràcter personal, i han de facilitar preferentment la prestació conjunta de serveis als interessats, i recull l'Esquema Nacional de Seguretat a l'article 156. Mentre que la Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques, recull a l'article 13, sobre drets de les persones en les seves relacions amb les administracions públiques, el relatiu a la protecció de dades de caràcter personal, i en particular a la seguretat i confidencialitat de les dades que figurin en els fitxers, els sistemes i les aplicacions de les administracions públiques.

En efecte, els ciutadans confien que els serveis públics disponibles pel mitjà electrònic es prestin en unes condicions de seguretat equivalents a les que troben quan s'acosten personalment a les oficines de l'Administració.

D'altra banda, les ciberamenaces, que constitueixen riscos que afecten singularment la seguretat nacional, s'han convertit en un potent instrument d'agressió contra les entitats públiques i els ciutadans en les seves relacions amb aquestes, de manera que la ciberseguretat figura entre els dotze àmbits prioritaris d'actuació de l'Estratègia de seguretat nacional com a instrument actualitzat per encarar el constant i profund canvi mundial en què estem immersos i com a garantia de l'actuació adequada d'Espanya en l'àmbit internacional. En particular, aquest àmbit d'actuació de ciberseguretat es refereix a la garantia de la seguretat dels sistemes d'informació i les xarxes de comunicacions i infraestructures comuns a totes les administracions públiques i al fet que s'ha de finalitzar la implantació de l'Esquema Nacional de Seguretat, previst a la Llei 11/2007, de 22 de juny. Aprofundint en la qüestió, l'Estratègia de ciberseguretat nacional «que utilitzen les administracions públiques tenen el nivell de ciberseguretat i resiliència adequat» i en la seva línia d'acció 2, titulada «Seguretat dels sistemes d'informació i telecomunicacions que suporten les administracions públiques», s'inclou la mesura relativa a «Assegurar la plena implantació de l'Esquema Nacional de Seguretat i articular els procediments necessaris per conèixer regularment l'estat de les principals variables de seguretat dels sistemes afectats».

Per tot això, i en particular atesa la ràpida evolució de les tecnologies d'aplicació i l'experiència derivada de la implantació de l'Esquema Nacional de Seguretat, aconsellen

l'actualització d'aquesta norma, l'abast i contingut de la qual s'orienta a precisar, aprofundir i contribuir al millor compliment dels manaments normatius, clarifica el paper del Centre Criptològic Nacional i del CCN-CERT, elimina la referència a INTECO, explicita i relaciona les instruccions tècniques de seguretat, i la declaració d'aplicabilitat, actualitza l'annex II, referit a les mesures de seguretat, i simplifica i concreta l'annex III, referit a l'auditoria de seguretat, modifica el glossari de termes que recull l'annex IV, modifica la redacció de la clàusula administrativa particular que conté l'annex V i finalitza amb l'establiment mitjançant una disposició transitòria d'un termini de vint-i-quatre mesos comptats a partir de l'entrada en vigor per a l'adequació dels sistemes al que disposa la modificació.

I en aquest sentit, es modifiquen l'apartat 1 de l'article 11, l'apartat 3 del 15, el títol del 18, el seu apartat 1 i s'hi afegeix un nou apartat 4, l'apartat a) del 19, l'apartat 2 del 24, el 27, mitjançant la introducció de dos nous apartats 4 i 5, el títol del 29, els seus apartats 1 i 2 i s'hi introdueix un nou apartat 3, els articles 35 i 36, l'apartat 1.a) del 37, els annexos II a V, s'elimina la disposició addicional segona, es modifica la numeració de les disposicions addicionals tercera i quarta i s'afegeix una nova disposició addicional quarta.

Tot això amb la finalitat esmentada i amb l'objectiu d'adequar-se al que preveu el Reglament núm. 910/2014, del Parlament Europeu i del Consell, de 23 de juliol de 2014, relatiu a la identificació electrònica i els serveis de confiança per a les transaccions electròniques en el mercat interior i pel qual es deroga la Directiva 1999/93/CE.

En virtut d'això, a proposta del ministre d'Hisenda i Administracions Públiques i de la ministra de la Presidència, d'acord amb el Consell d'Estat i amb la deliberació prèvia del Consell de Ministres en la reunió del dia 23 d'octubre de 2015,

DISPOSO:

Article únic. *Modificació del Reial decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat en l'àmbit de l'Administració electrònica.*

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, queda modificat en el sentit següent:

U. L'apartat 1 de l'article 11 queda redactat de la manera següent:

«Tots els òrgans superiors de les administracions públiques han de disposar formalment de la seva política de seguretat que articuli la gestió continuada de la seguretat, que ha de ser aprovada pel titular de l'òrgan superior corresponent. Aquesta política de seguretat s'ha d'establir d'acord amb els principis bàsics indicats i s'ha de desenvolupar aplicant els requisits mínims següents:

a) Organització i implantació del procés de seguretat.
b) Anàlisi i gestió dels riscos.
c) Gestió de personal.
d) Professionalitat.
e) Autorització i control dels accessos.
f) Protecció de les instal·lacions.
g) Adquisició de productes.
h) Seguretat per defecte.
i) Integritat i actualització del sistema.
j) Protecció de la informació emmagatzemada i en trànsit.
k) Prevenció davant altres sistemes d'informació interconnectats.
l) Registre d'activitat.
m) Incidents de seguretat.
n) Continuïtat de l'activitat.
o) Millora contínua del procés de seguretat.»

Dos. L'apartat 3 de l'article 15 queda redactat de la manera següent:

«3. Les administracions públiques han d'exigir, de manera objectiva i no discriminatòria, que les organitzacions que els prestin serveis de seguretat tinguin professionals qualificats i amb uns nivells idonis de gestió i maduresa en els serveis prestats.»

Tres. Es modifica l'article 18, el títol del qual passa a ser «Adquisició de productes de seguretat i contractació de serveis de seguretat», i els apartats 1 i 4 queden redactats de la manera següent:

«1. En l'adquisició de productes de seguretat de les tecnologies de la informació i comunicacions que hagin de ser utilitzats per les administracions públiques s'han d'utilitzar, de manera proporcionada a la categoria del sistema i el nivell de seguretat determinats, els que tinguin certificada la funcionalitat de seguretat relacionada amb l'objecte de la seva adquisició, tret en els casos en què les exigències de proporcionalitat quant als riscos assumits no ho justifiquin segons el parer del responsable de seguretat.»

«4. Per a la contractació de serveis de seguretat cal atenir-se al que disposen els apartats anteriors i l'article 15.»

Quatre. L'apartat a) de l'article 19 queda redactat de la manera següent:

«a) El sistema ha de proporcionar la mínima funcionalitat requerida perquè l'organització aconsegueixi els seus objectius.»

Cinc. L'apartat 2 de l'article 24 queda redactat de la manera següent:

«2. S'ha de disposar de procediments de gestió d'incidents de seguretat i de debilitats detectades en els elements del sistema d'informació. Aquests procediments han de cobrir els mecanismes de detecció, els criteris de classificació, els procediments d'anàlisi i resolució, així com les vies de comunicació a les parts interessades i el registre de les actuacions. Aquest registre s'ha d'utilitzar per a la millora contínua de la seguretat del sistema.»

Sis. S'afegeixen dos nous apartats 4 i 5 a l'article 27, redactats de la manera següent:

«4. La relació de mesures seleccionades de l'annex II s'ha de formalitzar en un document denominat declaració d'aplicabilitat, signat pel responsable de seguretat.

5. Les mesures de seguretat referenciades a l'annex II es poden reemplaçar per altres de compensatòries sempre que es justifiqui documentalment que protegeixen igual o millor el risc sobre els actius (annex I) i se satisfan els principis bàsics i els requisits mínims que preveuen els capítols II i III del Reial decret. Com a part integral de la declaració d'aplicabilitat s'ha d'indicar de manera detallada la correspondència entre les mesures compensatòries implantades i les mesures de l'annex II que compensen i el conjunt ha de ser objecte de l'aprovació formal per part del responsable de seguretat.»

Set. Es modifica l'article 29, el títol del qual passa a ser «Instruccions tècniques de seguretat i guies de seguretat», i queda redactat de la manera següent:

«1. Per al millor compliment del que estableix l'Esquema Nacional de Seguretat, el Centre Criptològic Nacional, en l'exercici de les seves competències, ha d'elaborar i difondre les corresponents guies de seguretat de les tecnologies de la informació i les comunicacions.

2. El Ministeri d'Hisenda i Administracions Públiques, a proposta del Comitè Sectorial d'Administració Electrònica que preveu l'article 40 de la Llei 11/2007, de 22 de juny, i a iniciativa del Centre Criptològic Nacional, ha d'aprovar les instruccions tècniques de seguretat de compliment obligat i s'han de publicar mitjançant una

resolució de la Secretaria d'Estat d'Administracions Públiques. Per a la redacció i el manteniment de les instruccions tècniques de seguretat s'han de constituir els grups de treball corresponents en els òrgans col·legiats amb competències en matèria d'administració electrònica.

3. Les instruccions tècniques de seguretat han de tenir en compte les normes harmonitzades a escala europea que siguin aplicables.»

Vuit. L'article 35 queda redactat de la manera següent:

«El Comitè Sectorial d'Administració Electrònica ha de recollir la informació relacionada amb l'estat de les principals variables de la seguretat en els sistemes d'informació a què es refereix el present Reial decret, de manera que permeti elaborar un perfil general de l'estat de la seguretat a les administracions públiques.

El Centre Criptològic Nacional ha d'articular els procediments necessaris per a la recollida i consolidació de la informació, així com els aspectes metodològics per al seu tractament i explotació, a través dels grups de treball corresponents que es constitueixin a l'efecte en el Comitè Sectorial d'Administració Electrònica i en la Comissió d'Estratègia TIC per a l'Administració General de l'Estat.»

Nou. A l'article 36 s'afegeix un segon paràgraf amb la redacció següent:

«Les administracions públiques han de notificar al Centre Criptològic Nacional els incidents que tinguin un impacte significatiu en la seguretat de la informació manejada i dels serveis prestats en relació amb la categorització de sistemes que recull l'annex I del present Reial decret.»

Deu. A l'article 37, l'apartat 1.a) queda redactat de la manera següent:

«a) Suport i coordinació per al tractament de vulnerabilitats i la resolució d'incidents de seguretat que tinguin l'Administració General de l'Estat, les administracions de les comunitats autònomes, les entitats que integren l'Administració local i les entitats de dret públic amb personalitat jurídica pròpia vinculades o dependents de qualsevol de les administracions indicades.

El CCN-CERT, a través del seu servei de suport tècnic i de coordinació, ha d'actuar amb la màxima celeritat davant de qualsevol agressió rebuda en els sistemes d'informació de les administracions públiques.

Per al compliment dels fins indicats en els paràgrafs anteriors es poden sol·licitar informes d'auditoria dels sistemes afectats, registres d'auditoria, configuracions i qualsevol altra informació que es consideri rellevant, així com els suports informàtics que es considerin necessaris per a la investigació de l'incident dels sistemes afectats, sense perjudici del que disposen la Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal, i la seva normativa de desplegament, així com de la possible confidencialitat de dades de caràcter institucional o organitzatiu.»

Onze. S'elimina la disposició addicional segona «Institut Nacional de Tecnologies de la Comunicació (INTECO) i organismes anàlegs», de manera que la disposició addicional tercera passa a ser la disposició addicional segona i la disposició addicional quarta passa a ser la disposició addicional tercera.

Dotze. S'afegeix una nova disposició addicional quarta redactada de la manera següent:

«Disposició addicional quarta. *Desenvolupament de l'Esquema Nacional de Seguretat.*

1. Sense perjudici de les propostes que pugui acordar el Comitè Sectorial d'Administració Electrònica segons el que estableix l'article 29, apartat 2, s'han de

desenvolupar les instruccions tècniques de seguretat següents, que han de ser de compliment obligat per part de les administracions públiques:

a) Informe de l'estat de la seguretat.
b) Notificació d'incidents de seguretat.
c) Auditoria de la seguretat.
d) Conformitat amb l'Esquema Nacional de Seguretat.
e) Adquisició de productes de seguretat.
f) Criptologia d'utilització a l'Esquema Nacional de Seguretat.
g) Interconnexió a l'Esquema Nacional de Seguretat.
h) Requisits de seguretat en entorns externalitzats.

2. L'aprovació d'aquestes instruccions s'ha de fer d'acord amb el procediment que estableix l'esmentat article 29, apartats 2 i 3.»

Tretze. La taula de l'apartat 2.4 de l'annex II queda redactada de la manera següent:

«Dimensions				Mesures de seguretat	
Afectades	B	M	A		
				org	**Marc organitzatiu**
categoria	aplica	=	=	org.1	Política de seguretat
categoria	aplica	=	=	org.2	Normativa de seguretat
categoria	aplica	=	=	org.3	Procediments de seguretat
categoria	aplica	=	=	org.4	Procés d'autorització
				op	**Marc operacional**
				op.pl	Planificació
categoria	aplica	+	++	op.pl.1	Anàlisi de riscos
categoria	aplica	+	++	op.pl.2	Arquitectura de seguretat
categoria	aplica	=	=	op.pl.3	Adquisició de nous components
D	n.a.	aplica	=	op.pl.4	Dimensionament/Gestió de capacitats
categoria	n.a.	n.a.	aplica	op.pl.5	Components certificats
				op.acc	Control d'accés
A T	aplica	=	=	op.acc.1	Identificació
I C A T	aplica	=	=	op.acc.2	Requisits d'accés
I C A T	n.a.	aplica	=	op.acc.3	Segregació de funcions i tasques
I C A T	aplica	=	=	op.acc.4	Procés de gestió de drets d'accés
I C A T	aplica	+	++	op.acc.5	Mecanisme d'autenticació
I C A T	aplica	+	++	op.acc.6	Accés local *(local logon)*
I C A T	aplica	+	=	op.acc.7	Accés remot *(remote login)*
				op.exp	Explotació
categoria	aplica	=	=	op.exp.1	Inventari d'actius
categoria	aplica	=	=	op.exp.2	Configuració de seguretat
categoria	n.a.	aplica	=	op.exp.3	Gestió de la configuració
categoria	aplica	=	=	op.exp.4	Manteniment
categoria	n.a.	aplica	=	op.exp.5	Gestió de canvis
categoria	aplica	=	=	op.exp.6	Protecció davant de codi perjudicial
categoria	n.a.	aplica	=	op.exp.7	Gestió d'incidents
T	aplica	+	++	op.exp.8	Registre de l'activitat dels usuaris
categoria	n.a.	aplica	=	op.exp.9	Registre de la gestió d'incidents
T	n.a.	n.a.	aplica	op.exp.10	Protecció dels registres d'activitat
categoria	aplica	+	=	op.exp.11	Protecció de claus criptogràfiques

«Dimensions				Mesures de seguretat	
Afectades	B	M	A		
				op.ext	Serveis externs
categoria	n.a.	aplica	=	op.ext.1	Contractació i acords de nivell de servei
categoria	n.a.	aplica	=	op.ext.2	Gestió diària
D	n.a.	n.a.	aplica	op.ext.9	Mitjans alternatius
				op.cont	Continuïtat del servei
D	n.a.	aplica	=	op.cont.1	Anàlisi d'impacte
D	n.a.	n.a.	aplica	op.cont.2	Pla de continuïtat
D	n.a.	n.a.	aplica	op.cont.3	Proves periòdiques
				op.mon	Monitorització del sistema
categoria	n.a.	aplica	=	op.mon.1	Detecció d'intrusió
categoria	n.a.	n.a.	aplica	op.mon.2	Sistema de mètriques
				mp	**Mesures de protecció**
				mp.if	Protecció de les instal·lacions i infraestructures
categoria	aplica	=	=	mp.if.1	Àrees separades i amb control d'accés
categoria	aplica	=	=	mp.if.2	Identificació de les persones
categoria	aplica	=	=	mp.if.3	Condicionament dels locals
D	aplica	+	=	mp.if.4	Energia elèctrica
D	aplica	=	=	mp.if.5	Protecció davant d'incendis
D	n.a.	aplica	=	mp.if.6	Protecció davant d'inundacions
categoria	aplica	=	=	mp.if.7	Registre d'entrada i sortida d'equipament
D	n.a.	n.a.	aplica	mp.if.9	Instal·lacions alternatives
				mp.per	Gestió del personal
categoria	n.a.	aplica	=	mp.per.1	Caracterització del lloc de treball
categoria	aplica	=	=	mp.per.2	Deures i obligacions
categoria	aplica	=	=	mp.per.3	Conscienciació
categoria	aplica	=	=	mp.per.4	Formació
D	n.a.	n.a.	aplica	mp.per.9	Personal alternatiu
				mp.eq	Protecció dels equips
categoria	aplica	+	=	mp.eq.1	Lloc de treball endreçat
A	n.a.	aplica	+	mp.eq.2	Bloqueig de lloc de treball
categoria	aplica	=	+	mp.eq.3	Protecció d'equips portàtils
D	n.a.	aplica	=	mp.eq.9	Mitjans alternatius
				mp.com	Protecció de les comunicacions
categoria	aplica	=	+	mp.com.1	Perímetre segur
C	n.a.	aplica	+	mp.com.2	Protecció de la confidencialitat
I A	aplica	+	++	mp.com.3	Protecció de l'autenticitat i de la integritat
categoria	n.a.	n.a.	aplica	mp.com.4	Segregació de xarxes
D	n.a.	n.a.	aplica	mp.com.9	Mitjans alternatius
				mp.si	Protecció dels suports d'informació
C	aplica	=	=	mp.si.1	Etiquetatge
I C	n.a.	aplica	+	mp.si.2	Criptografia
categoria	aplica	=	=	mp.si.3	Custòdia
categoria	aplica	=	=	mp.si.4	Transport
C	aplica	+	=	mp.si.5	Esborrament i destrucció
				mp.sw	Protecció de les aplicacions informàtiques
categoria	n.a.	aplica	=	mp.sw.1	Desenvolupament
categoria	aplica	+	++	mp.sw.2	Acceptació i posada en servei
				mp.info	Protecció de la informació
categoria	aplica	=	=	mp.info.1	Dades de caràcter personal
C	aplica	+	=	mp.info.2	Qualificació de la informació

«Dimensions				Mesures de seguretat	
Afectades	B	M	A		
C	n.a.	n.a.	aplica	mp.info.3	Xifratge
I A	aplica	+	++	mp.info.4	Signatura electrònica
T	n.a.	n.a.	aplica	mp.info.5	Segells de temps
C	aplica	=	=	mp.info.6	Neteja de documents
D	aplica	=	=	mp.info.9	Còpies de seguretat *(backup)*
				mp.s	Protecció dels serveis
categoria	aplica	=	=	mp.s.1	Protecció del correu electrònic
categoria	aplica	=	+	mp.s.2	Protecció de serveis i aplicacions web
D	n.a.	aplica	+	mp.s.8	Protecció davant de la denegació de servei
D	n.a.	n.a.	aplica	mp.s.9	Mitjans alternatius»

Catorze. Es modifiquen els apartats 3.4, 4.1.2, 4.1.5, 4.2.1, 4.2.5, 4.3.3, 4.3.7, 4.3.8, 4.3.9, 4.3.11, 4.4.2, 4.6.1, 4.6.2, 5.2.3, 5.3.3, 5.4.2, 5.4.3, 5.5.2, 5.5.5, 5.6.1, 5.7.4, 5.7.5, 5.7.7 i 5.8.2 de l'annex II del Reial decret, en els termes següents:

«3.4 Procés d'autorització [org.4].

dimensions	Totes		
categoria	bàsica	mitjana	alta
	aplica	=	=

S'ha d'establir un procés formal d'autoritzacions que cobreixi tots els elements del sistema d'informació:

a) Utilització d'instal·lacions, habituals i alternatives.
b) Entrada d'equips en producció, en particular, equips que involucrin criptografia.
c) Entrada d'aplicacions en producció.
d) Establiment d'enllaços de comunicacions amb altres sistemes.
e) Utilització de mitjans de comunicació, habituals i alternatius.
f) Utilització de suports d'informació.
g) Utilització d'equips mòbils. S'entén per equips mòbils ordinadors portàtils, PDA, o altres de naturalesa anàloga.
h) Utilització de serveis de tercers, sota contracte o conveni.»

«4.1.2 Arquitectura de seguretat [op.pl.2].

dimensions	Totes		
categoria	bàsica	mitjana	alta
	aplica	+	+

La seguretat del sistema ha de ser objecte d'un plantejament integral en què es detallin, almenys, els aspectes següents:

Categoria BÀSICA

a) Documentació de les instal·lacions:

1. Àrees.
2. Punts d'accés.

b) Documentació del sistema:

1. Equips.
2. Xarxes internes i connexions a l'exterior.
3. Punts d'accés al sistema (llocs de treball i consoles d'administració).

c) Esquema de línies de defensa:

1. Punts d'interconnexió a altres sistemes o a altres xarxes, en especial si es tracta d'Internet o xarxes públiques en general.
2. Tallafocs, DMZ, etc.
3. Utilització de tecnologies diferents per prevenir vulnerabilitats que puguin perforar simultàniament diverses línies de defensa.

d) Sistema d'identificació i autenticació d'usuaris:

1. Ús de claus concertades, contrasenyes, targetes d'identificació, biometria, o altres de naturalesa anàloga.
2. Ús de fitxers o directoris per autenticar l'usuari i determinar els seus drets d'accés.

Categoria MITJANA

e) Sistema de gestió, relatiu a la planificació, l'organització i el control dels recursos relatius a la seguretat de la informació.

Categoria ALTA

f) Sistema de gestió de seguretat de la informació amb actualització i aprovació periòdica.
g) Controls tècnics interns:

1. Validació de dades d'entrada, sortida i dades intermèdies.»

«4.1.5 Components certificats [op.pl.5].

dimensions	Totes		
categoria	bàsica	mitjana	alta
	no aplica	no aplica	aplica

Categoria ALTA

S'han d'utilitzar sistemes, productes o equips les funcionalitats de seguretat i el nivell dels quals hagin estat avaluats de conformitat amb normes europees o internacionals i els certificats dels quals estiguin reconeguts per l'Esquema Nacional d'Avaluació i Certificació de la Seguretat de les Tecnologies de la Informació.
Tenen la consideració de normes europees o internacionals, ISO/IEC 15408 o altres de naturalesa i qualitat anàlogues.
Una instrucció tècnica de seguretat ha de detallar els criteris exigibles.»

«4.2.1 Identificació [op.acc.1].

dimensions	A T		
nivell	baix	mitjà	alt
	aplica	=	=

La identificació dels usuaris del sistema s'ha de fer d'acord amb el que s'indica a continuació:

1. Es poden utilitzar com a identificador únic els sistemes d'identificació que prevegi la normativa aplicable.
2. Quan l'usuari tingui diferents rols davant del sistema (per exemple, com a ciutadà, com a treballador intern de l'organisme i com a administrador dels sistemes), ha de rebre identificadors singulars per a cadascun dels casos de manera que sempre quedin delimitats privilegis i registres d'activitat.
3. Cada entitat (usuari o procés) que accedeix al sistema ha de disposar d'un identificador singular de manera que:

a) Es pot saber qui rep i quins drets d'accés rep.
b) Es pot saber qui ha fet alguna cosa i què ha fet.

4. Els comptes d'usuari s'han de gestionar de la manera següent:

a) Cada compte ha d'estar associat a un identificador únic.
b) Els comptes han de ser inhabilitats en els casos següents: quan l'usuari deixa l'organització; quan l'usuari cessa en la funció per a la qual es requeria el compte d'usuari; o quan la persona que el va autoritzar dóna ordre en sentit contrari.
c) Els comptes s'han de retenir durant el període necessari per atendre les necessitats de traçabilitat dels registres d'activitat que hi estan associats. A aquest període se'l denomina període de retenció.

5. En els supòsits que preveu el capítol IV, relatiu a "Comunicacions electròniques", les parts intervinents s'han d'identificar d'acord amb els mecanismes que prevegi la legislació europea i nacional en la matèria, amb la següent correspondència entre els nivells de la dimensió d'autenticitat dels sistemes d'informació als quals es té accés i els nivells de seguretat (baix, substancial, alt) dels sistemes d'identificació electrònica que preveu el Reglament núm. 910/2014, del Parlament Europeu i del Consell, de 23 de juliol de 2014, relatiu a la identificació electrònica i els serveis de confiança per a les transaccions electròniques en el mercat interior i pel qual es deroga la Directiva 1999/93/CE:

– Si es requereix un nivell BAIX en la dimensió d'autenticitat (annex I): Nivell de seguretat baix, substancial o alt (article 8 del Reglament núm. 910/2014)
– Si es requereix un nivell MITJÀ en la dimensió d'autenticitat (annex I): Nivell de seguretat substancial o alt (article 8 del Reglament núm. 910/2014)
– Si es requereix un nivell ALT en la dimensió d'autenticitat (annex I): Nivell de seguretat alt (article 8 del Reglament núm. 910/2014).»

«4.2.5 Mecanisme d'autenticació [op.acc.5].

dimensions	ICAT		
nivell	baix	mitjà	alt
	aplica	+	++

Els mecanismes d'autenticació davant del sistema s'han d'adequar al nivell del sistema atenent les consideracions que segueixen, i es poden utilitzar els factors d'autenticació següents:

– "alguna cosa que se sap": contrasenyes o claus concertades.
– "alguna cosa que es té": components lògics (com ara certificats de programari) o dispositius físics (en expressió anglesa, *tokens).*
– "alguna cosa que s'és ": elements biomètrics.

Els factors anteriors es poden utilitzar de manera aïllada o combinar-se per generar mecanismes d'autenticació forta.

Les guies CCN-STIC han de desenvolupar els mecanismes concrets adequats per a cada nivell.

Les instàncies del factor o els factors d'autenticació que s'utilitzin en el sistema es denominen credencials.

Abans de proporcionar les credencials d'autenticació als usuaris, aquests s'han d'haver identificat i registrat de manera fidedigna davant el sistema o davant un proveïdor d'identitat electrònica reconegut per l'Administració. Es preveuen diverses possibilitats de registre dels usuaris:

– Mitjançant la presentació física de l'usuari i la verificació de la seva identitat d'acord amb la legalitat vigent, davant un funcionari habilitat per a això.

– De manera telemàtica, mitjançant DNI electrònic o un certificat electrònic qualificat.

– De manera telemàtica, utilitzant altres sistemes admesos legalment per a la identificació dels ciutadans dels que prevegi la normativa aplicable.

Nivell BAIX

a) Com a principi general, s'admet l'ús de qualsevol mecanisme d'autenticació sostingut en un sol factor.

b) En el cas que s'utilitzi com a factor "alguna cosa que se sap", s'han d'aplicar regles bàsiques de qualitat d'aquesta.

c) S'ha d'atendre la seguretat de les credencials de manera que:

1. Les credencials s'han d'activar una vegada estiguin sota el control efectiu de l'usuari.

2. Les credencials han d'estar sota el control exclusiu de l'usuari.

3. L'usuari ha de reconèixer que les ha rebut i que coneix i accepta les obligacions que implica la seva tinença, en particular, el deure de custòdia diligent, protecció de la seva confidencialitat i informació immediata en cas de pèrdua.

4. Les credencials s'han de canviar amb una periodicitat marcada per la política de l'organització, atenent la categoria del sistema al qual s'accedeix.

5. Les credencials s'han de retirar i deshabilitar quan l'entitat (persona, equip o procés) que auntentiquen acaba la seva relació amb el sistema.

Nivell MITJÀ

a) S'exigeix l'ús d'almenys dos factors d'autenticació.

b) En el cas d'utilització d'"alguna cosa que se sap" com a factor d'autenticació, s'han d'establir exigències rigoroses de qualitat i renovació.

c) Les credencials utilitzades s'han d'haver obtingut després d'un registre previ:

1. Presencial.

2. Telemàtic amb la utilització d'un certificat electrònic qualificat.

3. Telemàtic mitjançant una autenticació amb una credencial electrònica obtinguda després d'un registre previ presencial o telemàtic amb la utilització d'un certificat electrònic qualificat en un dispositiu qualificat de creació de signatura.

Nivell ALT

a) Les credencials s'han de suspendre després d'un període definit de no-utilització.

b) En el cas de l'ús d'utilització d'"alguna cosa que es té", es requereix l'ús d'elements criptogràfics de maquinari amb la utilització d'algoritmes i paràmetres acreditats pel Centre Criptològic Nacional.

c) Les credencials utilitzades s'han d'haver obtingut després d'un registre previ presencial o telemàtic amb la utilització d'un certificat electrònic qualificat en un dispositiu qualificat de creació de signatura.»

«4.3.3 Gestió de la configuració [op.exp.3].

dimensions	Totes		
categoria	bàsica	mitjana	alta
	no aplica	aplica	=

Categoria MITJANA

S'ha de gestionar de manera contínua la configuració dels components del sistema de manera que:

a) Es mantingui en tot moment la regla de "funcionalitat mínima" ([op.exp.2]).
b) Es mantingui en tot moment la regla de "seguretat per defecte" ([op.exp.2]).
c) El sistema s'adapti a les noves necessitats, prèviament autoritzades ([op.acc.4]).
d) El sistema reaccioni a vulnerabilitats reportades ([op.exp.4]).
e) El sistema reaccioni a incidents (vegeu [op.exp.7]).»

«4.3.7 Gestió d'incidents [op.exp.7].

dimensions	Totes		
categoria	bàsica	mitjana	alta
	no aplica	aplica	=

Categoria MITJANA

S'ha de disposar d'un procés integral per fer front als incidents que puguin tenir un impacte en la seguretat del sistema, incloent-hi:

a) Procediment de report d'esdeveniments de seguretat i debilitats, en què es detallin els criteris de classificació i l'escalat de la notificació.
b) Procediment de presa de mesures urgents, incloent-hi la detenció de serveis, l'aïllament del sistema afectat, la recollida d'evidències i la protecció dels registres, segons convingui al cas.
c) Procediment d'assignació de recursos per investigar les causes, analitzar les conseqüències i resoldre l'incident.
d) Procediments per informar les parts interessades, internes i externes.
e) Procediments per:

1. Prevenir que es repeteixi l'incident.
2. Incloure en els procediments d'usuari la identificació i la forma de tractar l'incident.
3. Actualitzar, estendre, millorar o optimitzar els procediments de resolució d'incidents.

La gestió d'incidents que afectin dades de caràcter personal ha de tenir en compte el que disposen la Llei orgànica 15/1999, de 13 de desembre, i les normes de desplegament, sense perjudici de complir, a més, les mesures que estableix aquest Reial decret.»

«4.3.8 Registre de l'activitat dels usuaris [op.exp.8].

dimensions	T		
nivell	baix	mitjà	alt
	aplica	+	++

S'han de registrar les activitats dels usuaris en el sistema, de manera que:

a) El registre ha d'indicar qui fa l'activitat, quan la fa i sobre quina informació.
b) S'ha d'incloure l'activitat dels usuaris i, especialment, la dels operadors i administradors quan puguin accedir a la configuració i actuar en el manteniment del sistema.
c) S'han de registrar les activitats efectuades amb èxit i els intents fracassats.
d) La determinació de quines activitats s'han de registrar i amb quins nivells de detall s'ha d'adoptar en vista de l'anàlisi de riscos feta sobre el sistema ([op.pl.1]).

Nivell BAIX

S'han d'activar els registres d'activitat en els servidors.

Nivell MITJÀ

S'han de revisar informalment els registres d'activitat per buscar patrons anormals.

Nivell ALT

S'ha de disposar d'un sistema automàtic de recol·lecció de registres i correlació d'esdeveniments; és a dir, una consola de seguretat centralitzada.»

«4.3.9 Registre de la gestió d'incidents [op.exp.9].

dimensions	Totes		
categoria	bàsica	mitjana	alta
	no aplica	aplica	=

Categoria MITJANA

S'han de registrar totes les actuacions relacionades amb la gestió d'incidents, de manera que:

a) S'han de registrar el report inicial, les actuacions d'emergència i les modificacions del sistema derivades de l'incident.
b) S'ha de registrar l'evidència que pugui sostenir, posteriorment, una demanda judicial, o fer-hi front, quan l'incident pugui portar a actuacions disciplinàries sobre el personal intern, sobre proveïdors externs o a la persecució de delictes. En la determinació de la composició i el detall d'aquestes evidències, s'ha de recórrer a assessorament legal especialitzat.
c) Com a conseqüència de l'anàlisi dels incidents, s'ha de revisar la determinació dels esdeveniments auditables.»

«4.3.11 Protecció de claus criptogràfiques [op.exp.11].

dimensions	Totes		
categoria	bàsica	mitjana	alta
	aplica	+	=

Les claus criptogràfiques s'han de protegir durant tot el seu cicle de vida: (1) generació, (2) transport al punt d'explotació, (3) custòdia durant l'explotació, (4) arxivament posterior a la seva retirada d'explotació activa i (5) destrucció final.

Categoria BÀSICA

a) Els mitjans de generació han d'estar aïllats dels mitjans d'explotació.
b) Les claus retirades d'operació que hagin de ser arxivades, ho han de ser en mitjans aïllats dels d'explotació.

Categoria MITJANA

a) S'han d'utilitzar programes avaluats o dispositius criptogràfics certificats de conformitat amb el que estableix [op.pl.5].
b) S'han d'utilitzar algoritmes acreditats pel Centre Criptològic Nacional.»

«4.4.2 Gestió diària [op.ext.2].

dimensions	Totes		
categoria	bàsica	mitjana	alta
	no aplica	aplica	=

Categoria MITJANA

Per a la gestió diària del sistema, s'han d'establir els punts següents:

a) Un sistema rutinari per mesurar el compliment de les obligacions de servei i el procediment per neutralitzar qualsevol desviació fora del marge de tolerància acordat ([op.ext.1]).
b) El mecanisme i els procediments de coordinació per portar a terme les tasques de manteniment dels sistemes afectats per l'acord.
c) El mecanisme i els procediments de coordinació en cas d'incidents i desastres (vegeu [op.exp.7]).»

«4.6.1 Detecció d'intrusió [op.mon.1].

dimensions	Totes		
categoria	bàsica	mitjana	alta
	no aplica	aplica	=

Categoria MITJANA

S'ha de disposar d'eines de detecció o de prevenció d'intrusió.»

«4.6.2 Sistema de mètriques [op.mon.2].

dimensions	Totes		
categoria	bàsica	mitjana	alta
	aplica	+	++

Categoria BÀSICA:

S'han de recopilar les dades necessàries atenent la categoria del sistema per conèixer el grau d'implantació de les mesures de seguretat que apliquin de les

detallades a l'annex II i, si s'escau, per proveir l'informe anual que requereix l'article 35.

Categoria MITJANA:

A més, s'han de recopilar dades per valorar el sistema de gestió d'incidents, que permetin conèixer

– Nombre d'incidents de seguretat tractats.
– Temps emprat per tancar el 50% dels incidents.
– Temps emprat per tancar el 90% dels incidents.

Categoria ALTA

S'han de recopilar dades per conèixer l'eficiència del sistema de seguretat TIC:

– Recursos consumits: hores i pressupost.»

«5.2.3 Conscienciació [mp.per.3].

dimensions	Totes		
categoria	bàsica	mitjana	alta
	aplica	=	=

S'han de dur a terme les accions necessàries per conscienciar regularment el personal sobre el seu paper i responsabilitat perquè la seguretat del sistema assoleixi els nivells exigits.
En particular, s'ha de recordar regularment:

a) La normativa de seguretat relativa al bon ús dels sistemes.
b) La identificació d'incidents, activitats o comportaments sospitosos que s'hagin de reportar per al seu tractament per personal especialitzat.
c) El procediment de report d'incidents de seguretat, ja siguin reals o falses alarmes.»

«5.3.3 Protecció de portàtils [mp.eq.3].

dimensions	Totes		
categoria	bàsica	mitjana	alta
	aplica	=	+

Categoria BÀSICA

Els equips que siguin susceptibles de sortir de les instal·lacions de l'organització i no es puguin beneficiar de la protecció física corresponent, amb un risc manifest de pèrdua o robatori, s'han de protegir adequadament.
Sense perjudici de les mesures generals que els afectin, s'han d'adoptar les següents:

a) S'ha de portar un inventari d'equips portàtils juntament amb una identificació de la persona que n'és responsable i un control regular del fet que està positivament sota el seu control.
b) S'ha d'establir un canal de comunicació per informar, el servei de gestió d'incidents, de pèrdues o sostraccions.
c) Quan un equip portàtil es connecti remotament a través de xarxes que no estan sota el control estricte de l'organització, l'àmbit d'operació del servidor ha de

limitar la informació i els serveis accessibles als mínims imprescindibles, i s'ha de requerir una autorització prèvia dels responsables de la informació i els serveis afectats. Aquest punt és aplicable a connexions a través d'Internet i altres xarxes que no siguin de confiança.

d) S'ha d'evitar, en la mesura en què sigui possible, que l'equip contingui claus d'accés remot a l'organització. Es consideren claus d'accés remot les que siguin capaces d'habilitar un accés a altres equips de l'organització, o altres de naturalesa anàloga.

Categoria ALTA

a) S'ha de dotar el dispositiu de detectors de violació que permetin saber si l'equip ha estat manipulat i activin els procediments previstos de gestió de l'incident.

b) La informació de nivell alt emmagatzemada en el disc s'ha de protegir mitjançant xifratge.»

«5.4.2 Protecció de la confidencialitat [mp.com.2].

dimensions	C		
nivell	baix	mitjà	alt
	no aplica	aplica	+

Nivell MITJÀ

a) S'han d'utilitzar xarxes privades virtuals quan la comunicació discorri per xarxes fora del propi domini de seguretat.

b) S'han d'utilitzar algoritmes acreditats pel Centre Criptològic Nacional.

Nivell ALT

a) S'han d'utilitzar, preferentment, dispositius de maquinari en l'establiment i la utilització de la xarxa privada virtual.

b) S'han d'utilitzar productes certificats de conformitat amb el que estableix [op.pl.5].»

«5.4.3 Protecció de l'autenticitat i de la integritat [mp.com.3].

dimensions	I A		
nivell	baix	mitjà	alt
	aplica	+	++

Nivell BAIX

a) S'ha d'assegurar l'autenticitat de l'altre extrem d'un canal de comunicació abans d'intercanviar informació (vegeu [op.acc.5]).

b) S'han de prevenir atacs actius, i garantir que almenys es detectaran i s'activaran els procediments previstos de tractament de l'incident. Es consideren atacs actius:

1. L'alteració de la informació en trànsit.
2. La injecció d'informació espúria.
3. El segrest de la sessió per una tercera part.

c) S'ha d'acceptar qualsevol mecanisme d'autenticació dels que prevegi la normativa aplicable.

Nivell MITJÀ

a) S'han d'utilitzar xarxes privades virtuals quan la comunicació discorri per xarxes fora del propi domini de seguretat.
b) S'han d'utilitzar algoritmes acreditats pel Centre Criptològic Nacional.
c) S'ha d'acceptar qualsevol mecanisme d'autenticació dels que prevegi la normativa aplicable. En cas d'ús de claus concertades s'han d'aplicar exigències mitjanes quant a la seva qualitat davant d'atacs d'endevinament, diccionari o força bruta.

Nivell ALT

a) S'ha de valorar positivament la utilització de dispositius de maquinari en l'establiment i la utilització de la xarxa privada virtual.
b) S'han d'utilitzar productes certificats de conformitat amb el que estableix [op.pl.5].
c) S'ha d'acceptar qualsevol mecanisme d'autenticació dels que prevegi la normativa aplicable. En cas d'ús de claus concertades s'han d'aplicar exigències altes quant a la seva qualitat davant d'atacs d'endevinament, diccionari o força bruta.»

«5.5.2 Criptografia [mp.si.2].

dimensions	I C		
nivell	baix	mitjà	alt
	no aplica	aplica	+

Aquesta mesura s'aplica, en particular, a tots els dispositius extraïbles. S'entenen per dispositius extraïbles els CD, DVD, discos USB, o altres de naturalesa anàloga.

Nivell MITJÀ

S'han d'aplicar mecanismes criptogràfics que garanteixin la confidencialitat i la integritat de la informació continguda.

Nivell ALT

a) S'han d'utilitzar algoritmes acreditats pel Centre Criptològic Nacional.
b) S'han d'utilitzar productes certificats de conformitat amb el que estableix [op.pl.5].»

«5.5.5 Esborrament i destrucció [mp.si.5].

dimensions	D		
nivell	baix	mitjà	alt
	no aplica	+	=

La mesura d'esborrament i destrucció de suports d'informació s'ha d'aplicar a tot tipus d'equips susceptibles d'emmagatzemar informació, incloent-hi mitjans electrònics i no electrònics.

Nivell BAIX

a) Els suports que s'hagin de reutilitzar per a una altra informació o alliberar a una altra organització han de ser objecte d'un esborrament segur del seu contingut.

Nivell MITJÀ

b) S'han de destruir de manera segura els suports, en els casos següents:

1. Quan la naturalesa del suport no permeti un esborrament segur.
2. Quan així ho requereixi el procediment associat al tipus d'informació continguda.

c) S'han d'utilitzar productes certificats de conformitat amb el que estableix ([op. pl.5]).»

«5.6.1 Desenvolupament d'aplicacions [mp.sw.1].

dimensions	Totes		
categoria	baix	mitjà	alt
	no aplica	aplica	=

Categoria MITJANA

a) El desenvolupament d'aplicacions s'ha de fer sobre un sistema diferent i separat del de producció, i no hi ha d'haver eines o dades de desenvolupament en l'entorn de producció.

b) S'ha d'aplicar una metodologia de desenvolupament reconeguda que:

1r Prengui en consideració els aspectes de seguretat al llarg de tot el cicle de vida.
2n Tracti específicament les dades utilitzades en proves.
3r Permeti la inspecció del codi font.
4t Inclogui normes de programació segura.

c) Els elements següents han de ser part integral del disseny del sistema:

1r Els mecanismes d'identificació i autenticació.
2n Els mecanismes de protecció de la informació tractada.
3r La generació i el tractament de pistes d'auditoria.

d) Les proves anteriors a la implantació o modificació dels sistemes d'informació no s'han de fer amb dades reals, llevat que s'asseguri el nivell de seguretat corresponent.»

«5.7.4 Signatura electrònica [mp.info.4].

dimensions	I A		
nivell	baix	mitjà	alt
	aplica	+	++

S'ha d'utilitzar la signatura electrònica com un instrument capaç de permetre la comprovació de l'autenticitat de la procedència i la integritat de la informació, i d'oferir les bases per evitar la repudiació.

La integritat i l'autenticitat dels documents s'han de garantir per mitjà de signatures electròniques amb els condicionants que es descriuen a continuació, proporcionats als nivells de seguretat requerits pel sistema.

En cas que s'utilitzin altres mecanismes de signatura electrònica subjectes a dret, el sistema ha d'incorporar mesures compensatòries suficients que ofereixin

garanties equivalents o superiors pel que fa a prevenció de la repudiació, amb l'ús del procediment que preveu el punt 5 de l'article 27.

Nivell BAIX

S'ha d'utilitzar qualsevol tipus de signatura electrònica dels que preveu la legislació vigent.

Nivell MITJÀ

a) Quan s'utilitzin sistemes de signatura electrònica avançada basats en certificats, aquests han de ser qualificats.
b) S'han d'utilitzar algoritmes i paràmetres acreditats pel Centre Criptològic Nacional.
c) S'ha de garantir la verificació i validació de la signatura electrònica durant el temps requerit per l'activitat administrativa que aquella suporti, sense perjudici que es pugui ampliar aquest període d'acord amb el que estableixi la política de signatura electrònica i de certificats que sigui aplicable. Per a aquesta finalitat:
d) S'ha d'adjuntar a la signatura, o s'ha de referenciar, tota la informació pertinent per a la seva verificació i validació:

1. Certificats.
2. Dades de verificació i validació.

e) L'organisme que sol·liciti documents signats per l'administrat ha de verificar i validar la signatura rebuda en el moment de la recepció, i ha d'annexar o referenciar sense ambigüitat la informació que descriuen els epígrafs 1 i 2 de l'apartat d).
f) La signatura electrònica de documents per part de l'Administració ha d'annexar o referenciar sense ambigüitat la informació que descriuen els epígrafs 1 i 2.

Nivell ALT

1. S'ha d'utilitzar signatura electrònica qualificada, amb la incorporació de certificats qualificats i dispositius qualificats de creació de signatura.
2. S'han d'utilitzar productes certificats de conformitat amb el que estableix [op.pl.5].»

«5.7.5 Segells de temps [mp.info.5].

dimensions	T		
nivell	baix	mitjà	alt
	no aplica	no aplica	aplica

Nivell ALT

Els segells de temps han de prevenir la possibilitat de la repudiació posterior:

1. Els segells de temps s'han d'aplicar a la informació que sigui susceptible de ser utilitzada com a evidència electrònica en el futur.
2. Les dades pertinents per a la verificació posterior de la data s'han de tractar amb la mateixa seguretat que la informació datada als efectes de disponibilitat, integritat i confidencialitat.
3. S'han de renovar regularment els segells de temps fins que la informació protegida ja no sigui requerida pel procés administratiu al qual dóna suport.
4. S'han d'utilitzar productes certificats (segons [op.pl.5]) o serveis externs admesos (vegeu [op.exp.10]).

5. S'han d'utilitzar "segells qualificats de temps electrònics" d'acord amb la normativa europea en la matèria.»

«5.7.7 Còpies de seguretat (backup) [mp.info.9].

dimensions	D		
nivell	baix	mitjà	alt
	aplica	=	=

S'han de fer còpies de seguretat que permetin recuperar dades perdudes, accidentalment o intencionadament amb una antiguitat determinada.

Aquestes còpies han de tenir el mateix nivell de seguretat que les dades originals pel que fa a integritat, confidencialitat, autenticitat i traçabilitat. En particular, s'ha de considerar la conveniència o necessitat, segons que correspongui, que les còpies de seguretat estiguin xifrades per garantir la confidencialitat.

Les còpies de seguretat han d'incloure:

g) Informació de treball de l'organització.

h) Aplicacions en explotació, incloent-hi els sistemes operatius.

i) Dades de configuració, serveis, aplicacions, equips, o altres de naturalesa anàloga.

j) Claus utilitzades per preservar la confidencialitat de la informació.»

«5.8.2 Protecció de serveis i aplicacions web [mp.s.2].

dimensions	Totes		
nivell	bàsica	mitjana	alta
	aplica	=	+

Els subsistemes dedicats a la publicació d'informació s'han de protegir davant de les amenaces que els són pròpies.

a) Quan la informació tingui algun tipus de control d'accés, s'ha de garantir la impossibilitat d'accedir a la informació obviant l'autenticació, en particular prenent mesures en els aspectes següents:

1r S'ha d'evitar que el servidor ofereixi accés als documents per vies alternatives al protocol determinat.

2n S'han de prevenir atacs de manipulació d'URL.

3r S'han de prevenir atacs de manipulació de fragments d'informació que s'emmagatzema en el disc dur del visitant d'una pàgina web a través del seu navegador, a petició del servidor de la pàgina, conegut en terminologia anglesa com a "cookies".

4t S'han de prevenir atacs d'injecció de codi.

b) S'han de prevenir intents d'escalat de privilegis.

c) S'han de prevenir atacs de "cross site scripting".

d) S'han de prevenir atacs de manipulació de programes o dispositius que fan una acció en representació d'altres, coneguts en terminologia anglesa com a "proxies", i sistemes especials d'emmagatzematge d'alta velocitat, coneguts en terminologia anglesa com a "caches".

Nivell BAIX

S'han d'utilitzar "certificats d'autenticació de lloc web" d'acord amb la normativa europea en la matèria.

Nivell ALT

S'han d'utilitzar "certificats qualificats d'autenticació del lloc web" d'acord amb la normativa europea en la matèria.»

Quinze. L'annex III, titulat «Auditoria de la seguretat», queda redactat de la manera següent:

«1. Objecte de l'auditoria.

1.1 La seguretat dels sistemes d'informació d'una organització s'ha d'auditar en els termes següents:

a) Que la política de seguretat defineix els rols i les funcions dels responsables de la informació, els serveis, els actius i la seguretat del sistema d'informació.
b) Que hi ha procediments per resoldre conflictes entre els responsables esmentats.
c) Que s'han designat persones per a aquests rols atenent el principi de "separació de funcions".
d) Que s'ha fet una anàlisi de riscos, amb revisió i aprovació anual.
e) Que es compleixen les recomanacions de protecció que descriu l'annex II, sobre mesures de seguretat, en funció de les condicions aplicables en cada cas.
f) Que hi ha un sistema de gestió de la seguretat de la informació, documentat i amb un procés regular d'aprovació per la direcció.

1.2 L'auditoria s'ha de basar en l'existència d'evidències que permetin sostenir objectivament el compliment dels punts esmentats:

a) Documentació dels procediments.
b) Registre d'incidents.
c) Examen del personal afectat: coneixement i praxi de les mesures que l'afecten.
d) Productes certificats. Es considera evidència suficient la utilització de productes que satisfacin el que estableix l'article 18 «Adquisició de productes i contractació de serveis de seguretat».

2. Nivells d'auditoria.

Els nivells d'auditoria que s'efectuen als sistemes d'informació són els següents:

2.1 Auditoria a sistemes de categoria BÀSICA.

a) Els sistemes d'informació de categoria BÀSICA, o inferior, no necessiten fer una auditoria. N'hi ha prou amb una autoavaluació efectuada pel mateix personal que administra el sistema d'informació, o en qui aquest delegui.
El resultat de l'autoavaluació ha d'estar documentat, i ha d'indicar si cada mesura de seguretat està implantada i subjecta a revisió regular i les evidències que sostenen la valoració anterior.
b) Els informes d'autoavaluació han de ser analitzats pel responsable de seguretat competent, que ha d'elevar les conclusions al responsable del sistema perquè adopti les mesures correctores adequades.

2.2 Auditoria a sistemes de categoria MITJANA O ALTA.

a) L'informe d'auditoria ha de dictaminar sobre el grau de compliment del present Reial decret, n'ha d'identificar les deficiències i ha de suggerir les possibles mesures correctores o complementàries que siguin necessàries, així com les recomanacions que es considerin oportunes. Ha d'incloure, igualment, els criteris

metodològics d'auditoria utilitzats, l'abast i l'objectiu de l'auditoria, i les dades, els fets i les observacions en què es basin les conclusions formulades.

b) Els informes d'auditoria han de ser analitzats pel responsable de seguretat competent, que ha de presentar les seves conclusions al responsable del sistema perquè adopti les mesures correctores adequades.

3. Interpretació.

La interpretació del present annex s'ha de fer segons el sentit propi de les seves paraules, en relació amb el context, antecedents històrics i legislatius, entre els quals figura el que disposa la instrucció tècnica CCN-STIC corresponent, atenent l'esperit i la finalitat d'aquelles.»

Setze. Es modifica l'annex IV, titulat: «Glossari». La definició de Gestió d'incidents queda de la manera següent:

«Gestió d'incidents. Pla d'acció per atendre els incidents que es donin. A més de resoldre'ls ha d'incorporar mesures de desenvolupament que permetin conèixer la qualitat del sistema de protecció i detectar tendències abans que es converteixin en grans problemes.»

Disset. L'annex V, relatiu al Model de clàusula administrativa particular, queda redactat de la manera següent:

«Clàusula administrativa particular.–En compliment del que disposen l'article 115.4 del Reial decret legislatiu 3/2011, de 14 de novembre, pel qual s'aprova el text refós de la Llei de contractes del sector públic, i l'article 18 del Reial decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat en l'àmbit de l'Administració electrònica, el licitador ha d'incloure una referència precisa, documentada i acreditativa del fet que els productes de seguretat, serveis, equips, sistemes, aplicacions o els seus components compleixen el que indica la mesura op.pl.5 sobre components certificats, que recull l'apartat 4.1.5 de l'annex II de l'esmentat Reial decret 3/2010, de 8 de gener.

Quan aquests siguin emprats per al tractament de dades de caràcter personal, el licitador també ha d'incloure el que estableix la disposició addicional única del 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.»

Disposició transitòria única. *Adequació de sistemes.*

Les entitats incloses dins l'àmbit d'aplicació del present Reial decret disposen d'un termini de vint-i-quatre mesos comptats a partir de la data de l'entrada en vigor del present Reial decret per adequar els seus sistemes al que s'hi disposa.

Disposició final única. *Entrada en vigor.*

Aquest Reial decret entra en vigor l'endemà de la publicació en el «Butlletí Oficial de l'Estat».

Oviedo, 23 d'octubre de 2015.

FELIPE R.

La vicepresidenta del Govern i ministra de la Presidència,
SORAYA SÁENZ DE SANTAMARÍA ANTÓN