I. DISPOSICIONS GENERALS

MINISTERI DE LA PRESIDÈNCIA

1330 *Reial decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat en l'àmbit de l'Administració electrònica.*

I

La necessària generalització de la societat de la informació és subsidiària, en gran mesura, de la confiança que generi en els ciutadans la relació a través de mitjans electrònics.

En l'àmbit de les administracions públiques, la consagració del dret a comunicar-s'hi a través de mitjans electrònics comporta una obligació correlativa d'aquestes, que té, com a premisses, la promoció de les condicions perquè la llibertat i la igualtat siguin reals i efectives, i la remoció dels obstacles que n'impedeixin o dificultin la plenitud, cosa que demana incorporar les peculiaritats que exigeixen una aplicació segura d'aquestes tecnologies.

A tot això dóna resposta l'article 42.2 de la Llei 11/2007, de 22 de juny, d'accés electrònic dels ciutadans als serveis públics, mitjançant la creació de l'Esquema Nacional de Seguretat, l'objecte del qual és l'establiment dels principis i requisits d'una política de seguretat en la utilització de mitjans electrònics que permeti la protecció adequada de la informació.

La finalitat de l'Esquema Nacional de Seguretat és la creació de les condicions necessàries de confiança en l'ús dels mitjans electrònics, a través de mesures per garantir la seguretat dels sistemes, les dades, les comunicacions i els serveis electrònics, que permeti als ciutadans i a les administracions públiques l'exercici de drets i el compliment de deures a través d'aquests mitjans.

L'Esquema Nacional de Seguretat persegueix fonamentar la confiança en el fet que els sistemes d'informació presten els seus serveis i custodien la informació d'acord amb les seves especificacions funcionals, sense interrupcions o modificacions fora de control, i sense que la informació pugui arribar al coneixement de persones no autoritzades. S'ha de desenvolupar i perfeccionar en paral·lel a l'evolució dels serveis i a mesura que es vagin consolidant els seu requisits i les infraestructures en què recolzen.

Actualment els sistemes d'informació de les administracions públiques estan fortament imbricats entre si i amb sistemes d'informació del sector privat: empreses i administrats. D'aquesta manera, la seguretat té un nou repte que va més enllà de l'assegurament individual de cada sistema. És per això que cada sistema ha de tenir clar el seu perímetre i els responsables de cada domini de seguretat s'han de coordinar efectivament per evitar «terres de ningú» i fractures que puguin danyar la informació o els serveis prestats.

En aquest context s'entén per seguretat de les xarxes i de la informació la capacitat de les xarxes o dels sistemes d'informació de resistir, amb un determinat nivell de confiança, els accidents o les accions il·lícites o malintencionades que comprometin la disponibilitat, autenticitat, integritat i confidencialitat de les dades emmagatzemades o transmeses i dels serveis que les esmentades xarxes i sistemes ofereixen o fan accessibles.

II

L'Esquema Nacional de Seguretat té presents les recomanacions de la Unió Europea (Decisió 2001/844/CE CECA, Euratom de la Comissió, de 29 de novembre de 2001, per la qual es modifica el seu Reglament intern, i Decisió 2001/264/CE del Consell, de 19 de març de 2001, per la qual s'adopten les normes de seguretat del Consell), la situació tecnològica de les diferents administracions públiques, així com els serveis electrònics de

què disposen, la utilització d'estàndards oberts i, de forma complementària, estàndards d'ús generalitzat pels ciutadans.

La seva articulació s'ha realitzat atenent la normativa nacional sobre Administració electrònica, protecció de dades de caràcter personal, signatura electrònica i document nacional d'identitat electrònic, Centre Criptològic Nacional, societat de la informació, reutilització de la informació en el sector públic i òrgans col·legiats responsables de l'Administració electrònica; així com la regulació de diferents instruments i serveis de l'Administració, les directrius i guies de l'OCDE i disposicions nacionals i internacionals sobre normalització.

La Llei 11/2007, de 22 de juny, possibilita i inspira aquesta norma, al desplegament de la qual coadjuva, en els aspectes de la seguretat dels sistemes de tecnologies de la informació en les administracions públiques, i contribueix al desenvolupament d'un instrument efectiu que permet garantir els drets dels ciutadans en l'Administració electrònica.

La Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal, i les seves normes de desplegament, determinen les mesures per a la protecció de les dades de caràcter personal. A més, aporten criteris per establir la proporcionalitat entre les mesures de seguretat i la informació a protegir.

La Llei 30/1992, de 26 de novembre, de règim jurídic de les administracions públiques i del procediment administratiu comú, referent legal imprescindible de qualsevol regulació administrativa, determina la configuració de nombrosos àmbits de confidencialitat administratius, diferents de la informació classificada i de les dades de caràcter personal, que necessiten ser materialment protegides. Així mateix determina el substrat legal de les comunicacions administratives i els seus requisits jurídics de validesa i eficàcia, que han de ser el suport dels requeriments tecnològics i de seguretat necessaris per projectar els seus efectes en les comunicacions realitzades per via electrònica.

La Llei 37/2007, de 16 de novembre, sobre reutilització de la informació del sector públic que determina la regulació bàsica del règim jurídic aplicable a la reutilització de documents elaborats en el sector públic, que configura un àmbit exceptuat de la seva aplicació, en el qual es troba la informació a la qual es refereix l'Esquema Nacional de Seguretat.

Juntament amb les disposicions indicades, han inspirat el contingut d'aquesta norma documents de l'Administració en matèria de seguretat electrònica, com ara els Criteris de seguretat, normalització i conservació, les Guies CCN-STIC de seguretat dels sistemes d'informació i comunicacions, la Metodologia i eines d'anàlisi i gestió de riscos o l'Esquema Nacional d'Interoperabilitat, també desplegat a l'empara del que disposa la Llei 11/2007, de 22 de juny.

III

Aquest Reial decret es limita a establir els principis bàsics i requisits mínims que, d'acord amb l'interès general, naturalesa i complexitat de la matèria regulada, permeten una protecció adequada de la informació i els serveis, cosa que exigeix incloure l'abast i procediment per gestionar la seguretat electrònica dels sistemes que tracten informació de les administracions públiques en l'àmbit de la Llei 11/2007, de 22 de juny. Amb això, s'aconsegueix un comú denominador normatiu, amb una regulació que no esgota totes les possibilitats de normació, i permet ser completada, mitjançant la regulació dels objectius, materialment no bàsics, que poden ser decidits per polítiques legislatives territorials.

Per donar compliment a tot això es determinen les dimensions de seguretat i els seus nivells, la categoria dels sistemes, les mesures de seguretat adequades i l'auditoria periòdica de la seguretat; s'implanta l'elaboració d'un informe per conèixer regularment l'estat de seguretat dels sistemes d'informació a què es refereix el present Reial decret, s'estableix el paper de la capacitat de resposta davant incidents de seguretat de la informació del Centre Criptològic Nacional, s'inclou un glossari de termes i es fa una referència expressa a la formació.

La norma s'estructura en deu capítols, quatre disposicions addicionals, una disposició transitòria, una disposició derogatòria i tres disposicions finals. Als quatre primers annexos dedicats a la categoria dels sistemes, les mesures de seguretat, l'auditoria de la seguretat i el glossari de termes, s'hi uneix un cinquè annex que estableix un model de clàusula administrativa particular a incloure en les prescripcions administratives dels contractes corresponents.

En aquest Reial decret es concep la seguretat com una activitat integral, en la qual no entren actuacions puntuals o tractaments conjunturals, ja que la debilitat d'un sistema la determina el seu punt més fràgil i, sovint, aquest punt és la coordinació entre mesures individualment adequades però deficientment acoblades. La informació tractada en els sistemes electrònics a què es refereix aquest Reial decret està protegida tenint en compte els criteris que estableix la Llei orgànica 15/1999, de 13 de desembre.

El present Reial decret s'aprova en aplicació del que disposa la disposició final vuitena de la Llei 11/2007, de 22 de juny, i, d'acord amb el que disposa l'article 42 apartat 3 i la disposició final primera de la norma esmentada, s'ha elaborat amb la participació de totes les administracions públiques a les quals és aplicable; ha rebut informe favorable de la Comissió Permanent del Consell Superior d'Administració Electrònica, la Conferència Sectorial d'Administració Pública i la Comissió Nacional d'Administració Local; i ha estat sotmès a l'informe previ de l'Agència Espanyola de Protecció de Dades. Així mateix, s'ha sotmès a l'audiència dels ciutadans segons les previsions que estableix l'article 24 de la Llei 50/1997, de 27 de novembre, del Govern.

En virtut d'això, a proposta 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 8 de gener de 2010,

DISPOSO:

CAPÍTOL I

Disposicions generals

Article 1. *Objecte.*

1. El present Reial decret té per objecte regular l'Esquema Nacional de Seguretat que estableix l'article 42 de la Llei 11/2007, de 22 de juny, i determinar la política de seguretat que s'ha d'aplicar en la utilització dels mitjans electrònics a què es refereix la Llei esmentada.

2. L'Esquema Nacional de Seguretat està constituït pels principis bàsics i requisits mínims requerits per a una protecció adequada de la informació. És aplicat per les administracions públiques per assegurar l'accés, integritat, disponibilitat, autenticitat, confidencialitat, traçabilitat i conservació de les dades, informacions i serveis utilitzats en mitjans electrònics que gestionin en l'exercici de les seves competències.

Article 2. *Definicions i estàndards.*

Als efectes que preveu aquest Reial decret, les definicions, paraules, expressions i termes s'han d'entendre en el sentit que indica el glossari de termes inclòs a l'annex IV.

Article 3. *Àmbit d'aplicació.*

L'àmbit d'aplicació del present Reial decret és el que estableix l'article 2 de la Llei 11/2007, de 22 de juny.

Estan exclosos de l'àmbit d'aplicació que indica el paràgraf anterior els sistemes que tracten informació classificada regulada per la Llei 9/1968, de 5 d'abril, de secrets oficials i normes de desplegament.

CAPÍTOL II

Principis bàsics

Article 4. *Principis bàsics de l'Esquema Nacional de Seguretat.*

L'objecte últim de la seguretat de la informació és assegurar que una organització administrativa pot complir els seus objectius utilitzant sistemes d'informació. En les decisions en matèria de seguretat s'han de tenir en compte els principis bàsics següents:

a) Seguretat integral.
b) Gestió de riscos.
c) Prevenció, reacció i recuperació.
d) Línies de defensa.
e) Reavaluació periòdica.
f) Funció diferenciada.

Article 5. *La seguretat com un procés integral.*

1. La seguretat s'entén com un procés integral constituït per tots els elements tècnics, humans, materials i organitzatius, relacionats amb el sistema. L'aplicació de l'Esquema Nacional de Seguretat està presidida per aquest principi, que exclou qualsevol actuació puntual o tractament conjuntural.
2. S'ha de prestar la màxima atenció a la conscienciació de les persones que intervenen en el procés i als seus responsables jeràrquics, perquè, ni la ignorància, ni la falta d'organització i coordinació, ni instruccions inadequades, siguin fonts de risc per a la seguretat.

Article 6. *Gestió de la seguretat basada en els riscos.*

1. L'anàlisi i gestió de riscos és part essencial del procés de seguretat i s'ha de mantenir permanentment actualitzat.
2. La gestió de riscos ha de permetre el manteniment d'un entorn controlat, minimitzant els riscos fins a nivells acceptables. La reducció d'aquests nivells s'ha de realitzar mitjançant el desplegament de mesures de seguretat, que ha d'establir un equilibri entre la naturalesa de les dades i els tractaments, els riscos a què estiguin exposats i les mesures de seguretat.

Article 7. *Prevenció, reacció i recuperació.*

1. La seguretat del sistema ha d'incloure els aspectes de prevenció, detecció i correcció, per aconseguir que les amenaces sobre aquest no es materialitzin, no afectin greument la informació que utilitza, o els serveis que s'hi presten.
2. Les mesures de prevenció han d'eliminar o, almenys, reduir, la possibilitat que les amenaces s'arribin a materialitzar amb perjudici per al sistema. Aquestes mesures de prevenció han de preveure, entre d'altres, la dissuasió i la reducció de l'exposició.
3. Les mesures de detecció han d'estar acompanyades de mesures de reacció, de forma que els incidents de seguretat es tallin a temps.
4. Les mesures de recuperació han de permetre la restauració de la informació i els serveis, de manera que es pugui fer front a les situacions en les quals un incident de seguretat inhabiliti els mitjans habituals.
5. Sense que hi hagi minva dels altres principis bàsics i requisits mínims establerts, el sistema ha de garantir la conservació de les dades i informacions en suport electrònic.

De la mateixa manera, el sistema ha de mantenir disponibles els serveis durant tot el cicle vital de la informació digital, a través d'una concepció i procediments que siguin la base per a la preservació del patrimoni digital.

Article 8. *Línies de defensa.*

1. El sistema ha de disposar d'una estratègia de protecció constituïda per múltiples capes de seguretat, disposada de forma que, quan una de les capes falli, permeti:

a) Guanyar temps per a una reacció adequada davant dels incidents que no s'han pogut evitar.
b) Reduir la probabilitat que el sistema sigui compromès en conjunt.
c) Minimitzar l'impacte final sobre el sistema.

2. Les línies de defensa han d'estar constituïdes per mesures de naturalesa organitzativa, física i lògica.

Article 9. *Reavaluació periòdica.*

Les mesures de seguretat s'han de reavaluar i actualitzar periòdicament, per adequar-ne l'eficàcia a la constant evolució dels riscos i sistemes de protecció, i es pot arribar fins i tot a un replantejament de la seguretat, si és necessari.

Article 10. *La seguretat com a funció diferenciada.*

En els sistemes d'informació s'ha de diferenciar el responsable de la informació, el responsable del servei i el responsable de la seguretat.
El responsable de la informació ha de determinar els requisits de la informació tractada; el responsable del servei ha de determinar els requisits dels serveis prestats; i el responsable de seguretat ha de determinar les decisions per satisfer els requisits de seguretat de la informació i dels serveis.
La responsabilitat de la seguretat dels sistemes d'informació ha d'estar diferenciada de la responsabilitat sobre la prestació dels serveis.
La política de seguretat de l'organització ha de detallar les atribucions de cada responsable i els mecanismes de coordinació i resolució de conflictes.

CAPÍTOL III

Requisits mínims

Article 11. *Requisits mínims de seguretat.*

1. Tots els òrgans superiors de les administracions públiques han de disposar formalment de la seva política de seguretat, que ha de ser aprovada pel titular de l'òrgan superior corresponent. Aquesta política de seguretat s'ha d'establir sobre la base dels 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.

2. Als efectes que indica l'apartat anterior, es consideren òrgans superiors els responsables directes de l'execució de l'acció del Govern, central, autonòmic o local, en un sector d'activitat específic, d'acord amb el que estableix la Llei 6/1997, de 14 d'abril, d'organització i funcionament de l'Administració General de l'Estat, i la Llei 50/1997, de 27 de novembre, del Govern; els estatuts d'autonomia corresponents i normes de desplegament; i la Llei 7/1985, de 2 d'abril, reguladora de les bases del règim local, respectivament.

Els municipis poden disposar d'una política de seguretat comuna elaborada per la diputació, cabildo, consell insular o òrgan unipersonal corresponent d'aquelles altres corporacions de caràcter representatiu a les quals correspongui el govern i l'administració autònoma de la província o, si s'escau, l'entitat comarcal corresponent a la qual pertanyin.

3. Tots aquests requisits mínims s'exigeixen en proporció als riscos identificats en cada sistema, i alguns poden no requerir-se en sistemes sense riscos significatius, i s'han de complir d'acord amb el que estableix l'article 27.

Article 12. *Organització i implantació del procés de seguretat.*

La seguretat ha de comprometre tots els membres de l'organització. La política de seguretat segons detalla l'annex II, secció 3.1, ha d'identificar uns responsables clars de vetllar pel seu compliment i ser coneguda per tots els membres de l'organització administrativa.

Article 13. *Anàlisi i gestió dels riscos.*

1. Cada organització que elabori i implanti sistemes per al tractament de la informació i les comunicacions ha de realitzar la seva pròpia gestió de riscos.

2. Aquesta gestió s'ha de fer per mitjà de l'anàlisi i el tractament dels riscos als quals està exposat el sistema. Sense perjudici del que disposa l'annex II, s'ha d'utilitzar alguna metodologia reconeguda internacionalment.

3. Les mesures adoptades per mitigar o suprimir els riscos han d'estar justificades i, en tot cas, hi ha d'haver una proporcionalitat entre aquestes i els riscos.

Article 14. *Gestió de personal.*

1. Tot el personal relacionat amb la informació i els sistemes ha de ser format i informat dels seus deures i obligacions en matèria de seguretat. Les seves actuacions han de ser supervisades per verificar que se segueixen els procediments establerts.

2. El personal relacionat amb la informació i els sistemes ha d'exercir i aplicar els principis de seguretat en l'exercici de la seva feina.

3. El significat i l'abast de l'ús segur del sistema s'ha de concretar i plasmar en unes normes de seguretat.

4. Per corregir, o exigir responsabilitats si s'escau, cada usuari que accedeixi a la informació del sistema ha d'estar identificat de forma única, de manera que se sàpiga, en tot moment, qui rep drets d'accés, de quin tipus són, i qui ha realitzat determinada activitat.

Article 15. *Professionalitat.*

1. La seguretat dels sistemes ha d'estar atesa, revisada i auditada per personal qualificat, dedicat i instruït en totes les fases del seu cicle de vida: instal·lació, manteniment, gestió d'incidències i desmantellament.

2. El personal de les administracions públiques ha de rebre la formació específica necessària per garantir la seguretat de les tecnologies de la informació aplicables als sistemes i serveis de l'Administració.

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

Article 16. *Autorització i control dels accessos.*

L'accés al sistema d'informació ha de ser controlat i limitat als usuaris, processos, dispositius i altres sistemes d'informació, degudament autoritzats, restringint l'accés a les funcions permeses.

Article 17. *Protecció de les instal·lacions.*

Els sistemes s'han d'instal·lar en àrees separades, dotades d'un procediment de control d'accés. Com a mínim, les sales han d'estar tancades i han de disposar d'un control de claus.

Article 18. *Adquisició de productes de seguretat.*

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 de valorar positivament els que tinguin certificada la funcionalitat de seguretat relacionada amb l'objecte de la seva adquisició.
2. La certificació que indica l'apartat anterior ha d'estar d'acord amb les normes i estàndards de més reconeixement internacional, en l'àmbit de la seguretat funcional.
3. L'Organisme de Certificació de l'Esquema Nacional d'Avaluació i Certificació de Seguretat de les Tecnologies de la Informació, constituït a l'empara del que disposa l'article 2.2.c) del Reial decret 421/2004, de 12 de març, i regulat per l'ordre PRE/2740/2007, de 19 de setembre, dins de les seves competències, ha de determinar el criteri a complir en funció de l'ús previst del producte a què es refereixi, en relació amb el nivell d'avaluació, altres certificacions de seguretat addicionals que es requereixin normativament, així com, excepcionalment, en els casos en què no existeixin productes certificats. El procés indicat s'ha d'efectuar tenint en compte els criteris i metodologies d'avaluació, determinats per les normes internacionals que recull l'ordre ministerial esmentada.

Article 19. *Seguretat per defecte.*

Els sistemes s'han de dissenyar i configurar de forma que garanteixin la seguretat per defecte:

a) El sistema ha de proporcionar la mínima funcionalitat requerida perquè l'organització només aconsegueixi als seus objectius, i no aconsegueixi cap altra funcionalitat addicional.
b) Les funcions d'operació, administració i registre d'activitat han de ser les mínimes necessàries, i s'ha d'assegurar que només són accessibles per les persones, o des d'emplaçaments o equips, autoritzats, i si s'escau es poden exigir restriccions d'horari i punts d'accés facultats.
c) En un sistema d'explotació s'han d'eliminar o desactivar, mitjançant el control de la configuració, les funcions que no siguin d'interès, les que siguin innecessàries i, fins i tot, les que siguin inadequades al fi que es persegueix.
d) L'ús ordinari del sistema ha de ser senzill i segur, de manera que una utilització insegura requereixi un acte conscient per part de l'usuari.

Article 20. *Integritat i actualització del sistema.*

1. Tot element físic o lògic requereix autorització formal prèvia a la seva instal·lació en el sistema.
2. S'ha de conèixer en tot moment l'estat de seguretat dels sistemes, en relació amb les especificacions dels fabricants, les vulnerabilitats i les actualitzacions que els afectin, i s'ha de reaccionar amb diligència per gestionar el risc en vista de l'estat de seguretat.

Article 21. *Protecció d'informació emmagatzemada i en trànsit.*

1. En l'estructura i organització de la seguretat del sistema, s'ha de prestar especial atenció a la informació emmagatzemada o en trànsit a través d'entorns insegurs. Tenen la consideració d'entorns insegurs els equips portàtils, assistents personals (PDA), dispositius perifèrics, suports d'informació i comunicacions sobre xarxes obertes o amb xifratge feble.

2. Formen part de la seguretat els procediments que assegurin la recuperació i conservació a llarg termini dels documents electrònics produïts per les administracions públiques en l'àmbit de les seves competències.

3. Tota informació en suport no electrònic, que hagi estat causa o conseqüència directa de la informació electrònica a què es refereix el present Reial decret, ha d'estar protegida amb el mateix grau de seguretat que aquesta. Per a això s'han d'aplicar les mesures que corresponguin a la naturalesa del suport en què es trobin, de conformitat amb les normes d'aplicació a la seguretat d'aquests.

Article 22. *Prevenció davant altres sistemes d'informació interconnectats.*

El sistema ha de protegir el perímetre, en particular, si es connecta a xarxes públiques. S'entén per xarxa pública de comunicacions la xarxa de comunicacions electròniques que s'utilitza, en la seva totalitat o principalment, per prestar serveis de comunicacions electròniques disponibles per al públic, de conformitat amb la definició que estableix l'apartat 26 de l'annex II de la Llei 32/2003, de 3 de novembre, general de telecomunicacions. En tot cas s'han d'analitzar els riscos derivats de la interconnexió del sistema, a través de xarxes, amb altres sistemes, i s'ha de controlar el seu punt d'unió.

Article 23. *Registre d'activitat.*

Amb la finalitat exclusiva d'aconseguir el compliment de l'objecte del present Reial decret, amb plenes garanties del dret a l'honor, a la intimitat personal i familiar i a la mateixa imatge dels afectats, i d'acord amb la normativa sobre protecció de dades personals, de funció pública o laboral, i altres disposicions que siguin aplicables, s'han de registrar les activitats dels usuaris, i retenir la informació necessària per monitorar, analitzar, investigar i documentar activitats indegudes o no autoritzades, i permetre identificar en cada moment la persona que actua.

Article 24. *Incidents de seguretat.*

1. S'ha d'establir un sistema de detecció i reacció davant de codi perjudicial.

2. S'han de registrar els incidents de seguretat que es produeixin i les accions de tractament que se segueixin. Aquests registres s'han d'utilitzar per a la millora contínua de la seguretat del sistema.

Article 25. *Continuïtat de l'activitat.*

Els sistemes han de disposar de còpies de seguretat i establir els mecanismes necessaris per garantir la continuïtat de les operacions, en cas de pèrdua dels mitjans habituals de treball.

Article 26. *Millora contínua del procés de seguretat.*

El procés integral de seguretat implantat ha de ser actualitzat i millorat de forma contínua. Per a això, s'han d'aplicar els criteris i mètodes reconeguts en la pràctica nacional i internacional relatius a gestió de les tecnologies de la informació.

Article 27. *Compliment de requisits mínims.*

1. Per donar compliment als requisits mínims que estableix el present Reial decret, les administracions públiques han d'aplicar les mesures de seguretat que indica l'annex II, tenint en compte:

a) Els actius que constitueixen el sistema.
b) La categoria del sistema, segons el que preveu l'article 43.
c) Les decisions que s'adoptin per gestionar els riscos identificats.

2. Quan un sistema al qual afecti el present Reial decret utilitzi dades de caràcter personal li és aplicable el que disposa la Llei orgànica 15/1999, de 13 de desembre, i normativa de desplegament, sense perjudici dels requisits que estableix l'Esquema Nacional de Seguretat.

3. Les mesures a què es refereixen els apartats 1 i 2 tenen la condició de mínims exigibles, i poden ser ampliats per causa de la concurrència indicada o del prudent arbitri del responsable de la informació, tenint en compte l'estat de la tecnologia, la naturalesa dels serveis prestats i la informació manejada, i els riscos a què estan exposats.

Article 28. *Infraestructures i serveis comuns.*

La utilització d'infraestructures i serveis comuns reconeguts en les administracions públiques ha de facilitar el compliment dels principis bàsics i els requisits mínims exigits en el present Reial decret en condicions de millor eficiència. Els supòsits concrets d'utilització d'aquestes infraestructures i serveis comuns són determinats per cada Administració.

Article 29. *Guies de seguretat.*

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.

Article 30. *Sistemes d'informació no afectats.*

Les administracions públiques poden determinar els sistemes d'informació als quals no els sigui aplicable el que disposa el present de Reial decret si es tracta de sistemes no relacionats amb l'exercici de drets ni amb el compliment de deures per mitjans electrònics ni amb l'accés per mitjans electrònics dels ciutadans a la informació i al procediment administratiu, d'acord amb el que preveu la Llei 11/2007, de 22 de juny.

CAPÍTOL IV

Comunicacions electròniques

Article 31. *Condicions tècniques de seguretat de les comunicacions electròniques.*

1. Les condicions tècniques de seguretat de les comunicacions electròniques pel que fa a la constància de la transmissió i recepció, de les seves dates, del contingut íntegre de les comunicacions i la identificació fidedigna del remitent i destinatari d'aquestes, segons el que estableix la Llei 11/2007, de 22 de juny, s'han d'implementar d'acord amb el que estableix l'Esquema Nacional de Seguretat.

2. Les comunicacions realitzades en els termes que indica l'apartat anterior tenen el valor i l'eficàcia jurídica que correspongui a la seva respectiva naturalesa, de conformitat amb la legislació que sigui aplicable.

Article 32. *Requeriments tècnics de notificacions i publicacions electròniques.*

1. Les notificacions i publicacions electròniques de resolucions i actes administratius s'han de realitzar de forma que compleixin, d'acord amb el que estableix el present Reial decret, les exigències tècniques següents:

a) Assegurin l'autenticitat de l'organisme que ho publiqui.
b) Assegurin la integritat de la informació publicada.
c) Deixin constància de la data i l'hora de la posada a disposició de l'interessat de la resolució o acte objecte de publicació o notificació, així com de l'accés al seu contingut.
d) Assegurin l'autenticitat del destinatari de la publicació o notificació.

Article 33. *Signatura electrònica.*

1. Els mecanismes de signatura electrònica s'han d'aplicar en els termes que indica l'annex II d'aquesta norma i d'acord amb el que preceptua la política de signatura electrònica i de certificats, segons estableix l'Esquema Nacional d'Interoperabilitat.
2. La política de signatura electrònica i de certificats ha de concretar els processos de generació, validació i conservació de signatures electròniques, així com les característiques i requisits exigibles als sistemes de signatura electrònica, els certificats, els serveis de segellament de temps, i altres elements de suport de les signatures, sense perjudici del que preveu l'annex II, que s'ha d'adaptar a cada circumstància.

CAPÍTOL V

Auditoría de la seguretat

Article 34. *Auditoría de la seguretat.*

1. Els sistemes d'informació a què es refereix el present Reial decret han de ser objecte d'una auditoria regular ordinària, almenys cada dos anys, que verifiqui el compliment dels requeriments del present Esquema Nacional de Seguretat.

Amb caràcter extraordinari, s'ha de realitzar l'auditoria esmentada sempre que es produeixin modificacions substancials en el sistema d'informació, que puguin repercutir en les mesures de seguretat requerides. La realització de l'auditoria extraordinària determina la data de còmput per al càlcul dels dos anys, establerts per a la realització de l'auditoria regular ordinària següent, indicats en el paràgraf anterior.

2. Aquesta auditoria s'ha de realitzar en funció de la categoria del sistema, determinada segons el que disposa l'annex I i d'acord amb el que preveu l'annex III.
3. En el marc del que disposa l'article 39 de la Llei 11/2007, de 22 de juny, l'auditoria ha d'aprofundir en els detalls del sistema fins al nivell que consideri que proporciona evidència suficient i rellevant, dins de l'abast establert per a l'auditoria.
4. En la realització d'aquesta auditoria s'han d'utilitzar els criteris, mètodes de treball i de conducta generalment reconeguts, així com la normalització nacional i internacional aplicables a aquest tipus d'auditories de sistemes d'informació.
5. L'informe d'auditoria ha de dictaminar sobre el grau de compliment del present Reial decret, identificar les seves deficiències i suggerir les possibles mesures correctores o complementàries necessàries, així com les recomanacions que es considerin oportunes. Igualment, ha d'incloure els criteris metodològics d'auditoria utilitzats, l'abast i l'objectiu de l'auditoria, i les dades, fets i observacions en què es basin les conclusions formulades.
6. Els informes d'auditoria s'han de presentar al responsable del sistema i al responsable de seguretat competents. Aquests informes han de ser analitzats per aquest últim, que n'ha de presentar les conclusions al responsable del sistema perquè adopti les mesures correctores adequades.
7. En el cas dels sistemes de categoria ALTA, vist el dictamen d'auditoria, el responsable del sistema pot acordar la retirada d'operació d'alguna informació, d'algun servei o del sistema en la seva totalitat, durant el temps que estimi prudent i fins a satisfer les modificacions prescrites.
8. Els informes d'auditoria poden ser requerits pels responsables de cada organització amb competències sobre seguretat de les tecnologies de la informació.

CAPITULO VI

Estat de seguretat dels sistemes

Article 35. *Informe de l'estat de la seguretat.*

El Comitè Sectorial d'Administració Electrònica ha d'articular els procediments necessaris per conèixer regularment l'estat de les principals variables de la seguretat en els sistemes d'informació a què es refereix el present Reial decret, de forma que permeti elaborar un perfil general de l'estat de la seguretat a les administracions públiques.

CAPÍTOL VII

Resposta a incidents de seguretat

Article 36. *Capacitat de resposta a incidents de seguretat de la informació.*

El Centre Criptològic Nacional (CCN) ha d'articular la resposta als incidents de seguretat a l'entorn de l'estructura denominada CCN-CERT (Centre Criptològic Nacional-Computer Emergency Reaction Team), que ha d'actuar sense perjudici de les capacitats de resposta a incidents de seguretat que pugui tenir cada administració pública i de la funció de coordinació a nivell nacional i internacional del CCN.

Article 37. *Prestació de serveis de resposta a incidents de seguretat a les administracions públiques.*

1. D'acord amb el que preveu l'article 36, el CCN-CERT ha de prestar a les administracions públiques els serveis següents:

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 els informes d'auditoria dels sistemes afectats.

b) Recerca i divulgació de les millors pràctiques sobre seguretat de la informació entre tots els membres de les administracions públiques. Amb aquesta finalitat, les sèries de documents CCN-STIC (Centre Criptològic Nacional-Seguretat de les Tecnologies d'Informació i Comunicacions), elaborades pel Centre Criptològic Nacional, han d'oferir normes, instruccions, guies i recomanacions per aplicar l'Esquema Nacional de Seguretat i per garantir la seguretat dels sistemes de tecnologies de la informació en l'Administració.

c) Formació destinada al personal de l'Administració especialista en el camp de la seguretat de les tecnologies de la informació, per tal de facilitar l'actualització de coneixements del personal de l'Administració i d'aconseguir la sensibilització i millora de les seves capacitats per a la detecció i gestió d'incidents.

d) Informació sobre vulnerabilitats, alertes i avisos de noves amenaces als sistemes d'informació, recopilades de diverses fonts de reconegut prestigi, incloses les pròpies.

2. El CCN ha de desenvolupar un programa que ofereixi la informació, formació, recomanacions i eines necessàries perquè les administracions públiques puguin desenvolupar les seves pròpies capacitats de resposta a incidents de seguretat, i en el qual aquell ha de ser coordinador a nivell públic estatal.

CAPÍTOL VIII

Normes de conformitat

Article 38. *Seus i registres electrònics.*

La seguretat de les seus i registres electrònics, així com la de l'accés electrònic dels ciutadans als serveis públics es regeix pel que estableix l'Esquema Nacional de Seguretat.

Article 39. *Cicle de vida de serveis i sistemes.*

Les especificacions de seguretat s'han d'incloure en el cicle de vida dels serveis i sistemes, acompanyades dels corresponents procediments de control.

Article 40. *Mecanismes de control.*

Cada òrgan de l'Administració pública o entitat de dret públic ha d'establir els seus mecanismes de control per garantir de forma real i efectiva el compliment de l'Esquema Nacional de Seguretat.

Article 41. *Publicació de conformitat.*

Els òrgans i entitats de dret públic han de donar publicitat en les corresponents seus electròniques a les declaracions de conformitat, i als distintius de seguretat dels quals siguin creditors, obtinguts respecte al compliment de l'Esquema Nacional de Seguretat.

CAPÍTOL IX

Actualització

Article 42. *Actualització permanent.*

L'Esquema Nacional de Seguretat s'ha de mantenir actualitzat de manera permanent. S'ha de desenvolupar i perfeccionar al llarg del temps, en paral·lel al progrés dels serveis d'Administració electrònica, de l'evolució tecnològica i nous estàndards internacionals sobre seguretat i auditoria en els sistemes i tecnologies de la informació i a mesura que es vagin consolidant les infraestructures en què recolza.

CAPÍTOL X

Categorització dels sistemes d'informació

Article 43. *Categories.*

1. La categoria d'un sistema d'informació, en matèria de seguretat, ha de modular l'equilibri entre la importància de la informació que utilitza, els serveis que ofereix i l'esforç de seguretat requerit, en funció dels riscos als quals està exposat, sota el criteri del principi de proporcionalitat.
2. La determinació de la categoria que indica l'apartat anterior s'efectua en funció de la valoració de l'impacte que tindria un incident que afectés la seguretat de la informació o dels serveis amb perjudici per a la disponibilitat, autenticitat, integritat, confidencialitat o traçabilitat, com a dimensions de seguretat, seguint el procediment que estableix l'annex I.
3. La valoració de les conseqüències d'un impacte negatiu sobre la seguretat de la informació i dels serveis s'ha d'efectuar atenent la seva repercussió en la capacitat de l'organització per a l'assoliment dels seus objectius, la protecció dels seus actius, el compliment de les seves obligacions de servei, el respecte de la legalitat i els drets dels ciutadans.

Article 44. *Facultats.*

1. La facultat per efectuar les valoracions a les quals es refereix l'article 43, així com la modificació posterior, si s'escau, correspon, dins de l'àmbit de la seva activitat, al responsable de cada informació o servei.
2. La facultat per determinar la categoria del sistema correspon al seu responsable.

Disposició addicional primera. *Formació.*

El personal de les administracions públiques ha de rebre, d'acord amb el que preveu la disposició addicional segona de la Llei 11/2007, de 22 de juny, la formació necessària per garantir el coneixement del present Esquema Nacional de Seguretat, i amb aquest fi els òrgans responsables han de disposar el que sigui necessari perquè la formació sigui una realitat efectiva.

Disposició addicional segona. *Institut Nacional de Tecnologies de la Comunicació (INTECO) i organismes anàlegs.*

L'Institut Nacional de Tecnologies de la Comunicació (INTECO), com a centre d'excel·lència promogut pel Ministeri d'Indústria, Turisme i Comerç per al desenvolupament de la societat del coneixement, pot desenvolupar projectes d'innovació i programes de recerca adreçats a la millor implantació de les mesures de seguretat que preveu el present Reial decret.

Així mateix, les administracions públiques poden disposar d'entitats anàlogues per portar a terme les esmentades activitats o altres d'addicionals en l'àmbit de les seves competències.

Disposició addicional tercera. *Comitè de Seguretat de la Informació de les Administracions Públiques.*

El Comitè de Seguretat de la Informació de les Administracions Públiques, dependent del Comitè Sectorial d'Administració electrònica, ha de tenir un representant de cadascuna de les entitats presents a l'esmentat Comitè Sectorial. Té funcions de cooperació en matèries comunes relacionades amb l'adequació i implantació del que preveuen l'Esquema Nacional de Seguretat i les normes, instruccions, guies i recomanacions dictades per a la seva aplicació.

Disposició addicional quarta. *Modificació del Reglament de desplegament de la Llei orgànica 15/1999, de protecció de dades de caràcter personal, aprovat pel Reial decret 1720/2007, de 21 de desembre.*

Es modifica la lletra b) de l'apartat 5 de l'article 81 del Reglament de desplegament de la Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal, aprovat pel Reial decret 1720/2007, de 21 de desembre, que passa a tenir la redacció següent:

> «b) Es tracta de fitxers o tractaments que de forma incidental o accessòria continguin aquelles dades sense tenir relació amb la seva finalitat.»

Disposició transitòria. *Adequació de sistemes.*

1. Els sistemes existents a l'entrada en vigor del present Reial decret s'han d'adequar a l'Esquema Nacional de Seguretat de forma que permetin el compliment del que estableix la disposició final tercera de la Llei 11/2007, de 22 de juny. Els nous sistemes han d'aplicar el que estableix el present Reial decret des de la seva concepció.
2. Si al cap de dotze mesos de l'entrada en vigor de l'Esquema Nacional de Seguretat hi ha circumstàncies que impedeixen la plena aplicació del que s'hi exigeix, s'ha de disposar d'un pla d'adequació que marqui els terminis d'execució, els quals en cap cas no poden ser superiors a 48 mesos des de l'entrada en vigor.

El pla indicat en el paràgraf anterior s'ha d'elaborar amb l'antelació suficient i ha de ser aprovat pels òrgans superiors competents.

3. Mentre l'òrgan superior competent no hagi aprovat una política de seguretat són aplicables les polítiques de seguretat que puguin existir a nivell d'òrgan directiu.

Disposició derogatòria única.

Queden derogades les disposicions del mateix rang o inferior que s'oposin al que disposa el present Reglament.

Disposició final primera. *Títol habilitador.*

El present Reial decret es dicta en virtut del que estableix l'article 149.1.18a de la Constitució, que atribueix a l'Estat la competència sobre les bases del règim jurídic de les administracions públiques.

Disposició final segona. *Desplegament normatiu.*

S'autoritza el titular del Ministeri de la Presidència per dictar les disposicions necessàries per a l'aplicació i desplegament del que estableix el present Reial decret, sense perjudici de les competències de les comunitats autònomes de desplegament i execució de la legislació bàsica de l'Estat.

Disposició final tercera. *Entrada en vigor.*

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

Madrid, 8 de gener de 2010.

JUAN CARLOS R.

La vicepresidenta primera del Govern
i ministra de la Presidència,
MARÍA TERESA FERNÁNDEZ DE LA VEGA SANZ

ANNEXOS

ANNEX I

Categories dels sistemes

1. Fonaments per a la determinació de la categoria d'un sistema.

La determinació de la categoria d'un sistema es basa en la valoració de l'impacte que tindria sobre l'organització un incident que afectés la seguretat de la informació o dels sistemes, amb repercussió en la capacitat organitzativa per:

a) Aconseguir els seus objectius.
b) Protegir els actius a càrrec seu.
c) Complir les seves obligacions diàries de servei.
d) Respectar la legalitat vigent.
e) Respectar els drets de les persones.

La determinació de la categoria d'un sistema es realitza d'acord amb el que estableix el present Reial decret, i és aplicable a tots els sistemes utilitzats per a la prestació dels serveis de l'Administració electrònica i suport del procediment administratiu general.

2. Dimensions de la seguretat.

A fi de poder determinar l'impacte que tindria sobre l'organització un incident que afectés la seguretat de la informació o dels sistemes, i de poder establir la categoria del sistema, s'han de tenir en compte les dimensions de la seguretat següents, que han de ser identificades per les seves inicials corresponents en majúscules:

a) Disponibilitat [D].
b) Autenticitat [A].
c) Integritat [I].
d) Confidencialitat [C].
e) Traçabilitat [T].

3. Determinació del nivell requerit en una dimensió de seguretat.

Una informació o un servei es poden veure afectats en una o més de les seves dimensions de seguretat. Cada dimensió de seguretat afectada s'ha d'adscriure a un dels nivells següents: BAIX, MITJÀ o ALT. Si una dimensió de seguretat no es veu afectada, no s'ha d'adscriure a cap nivell.

a) Nivell BAIX. S'utilitza quan les conseqüències d'un incident de seguretat que afecti alguna de les dimensions de seguretat suposin un perjudici limitat sobre les funcions de l'organització, sobre els seus actius o sobre els individus afectats.
S'entén per perjudici limitat:

1r La reducció de forma apreciable de la capacitat de l'organització per atendre eficaçment les seves obligacions corrents, encara que aquestes se segueixin portant a terme.
2n El patiment d'un dany menor pels actius de l'organització.
3r L'incompliment formal d'alguna llei o regulació, que tingui caràcter de reparable.
4t Causar un perjudici menor a algun individu, que tot i ser molest pugui ser fàcilment reparable.
5è Altres de naturalesa anàloga.

b) Nivell MITJÀ. S'utilitza quan les conseqüències d'un incident de seguretat que afecti alguna de les dimensions de seguretat suposin un perjudici greu sobre les funcions de l'organització, sobre els seus actius o sobre els individus afectats.

S'entén per perjudici greu:

1r La reducció significativa de la capacitat de l'organització per atendre eficaçment les seves obligacions fonamentals, encara que aquestes se segueixin portant a terme.
2n El patiment d'un dany significatiu pels actius de l'organització.
3r L'incompliment material d'alguna llei o regulació, o l'incompliment formal que no tingui caràcter de reparable.
4t Causar un perjudici significatiu a algun individu, de reparació difícil.
5è Altres de naturalesa anàloga.

c) Nivell ALT. S'utilitza quan les conseqüències d'un incident de seguretat que afecti alguna de les dimensions de seguretat suposin un perjudici molt greu sobre les funcions de l'organització, sobre els seus actius o sobre els individus afectats.
S'entén per perjudici molt greu:

1r L'anul·lació de la capacitat de l'organització per atendre alguna de les seves obligacions fonamentals i que aquestes se segueixin portant a terme.
2n El patiment d'un dany molt greu, i fins i tot irreparable, pels actius de l'organització.
3r L'incompliment greu d'alguna llei o regulació.
4t Causar un perjudici greu a algun individu, de reparació difícil o impossible.
5è Altres de naturalesa anàloga.

Quan un sistema utilitzi informacions diferents i presti serveis diferents, el nivell del sistema en cada dimensió ha de ser el més gran dels establerts per a cada informació i cada servei.

4. Determinació de la categoria d'un sistema d'informació.

1. Es defineixen tres categories: BÀSICA, MITJANA i ALTA.

a) Un sistema d'informació és de categoria ALTA si alguna de les seves dimensions de seguretat assoleix el nivell ALT.
b) Un sistema d'informació és de categoria MITJANA si alguna de les seves dimensions de seguretat assoleix el nivell MITJÀ, i cap assoleix un nivell superior.
c) Un sistema d'informació és de categoria BÀSICA si alguna de les seves dimensions de seguretat assoleix el nivell BAIX, i cap assoleix un nivell superior.

2. La determinació de la categoria d'un sistema sobre la base del que indica l'apartat anterior no implica que s'alteri, per aquest fet, el nivell de les dimensions de seguretat que no han influït en la determinació de la seva categoria.

5. Seqüència d'actuacions per determinar la categoria d'un sistema:

1. Identificació del nivell corresponent a cada informació i servei, en funció de les dimensions de seguretat, tenint en compte el que estableix l'apartat 3.
2. Determinació de la categoria del sistema, segons el que estableix l'apartat 4.

ANNEX II

Mesures de seguretat

1. Disposicions generals

1. Per aconseguir el compliment dels principis bàsics i requisits mínims establerts, s'apliquen les mesures de seguretat que indica aquest annex, les quals són proporcionals a:

a) Les dimensions de seguretat rellevants en el sistema a protegir.
b) La categoria del sistema d'informació a protegir.

2. Les mesures de seguretat es divideixen en tres grups:

a) Marc organitzatiu [org]. Constituït pel conjunt de mesures relacionades amb l'organització global de la seguretat.

b) Marc operacional [op]. Format per les mesures que s'han de prendre per protegir l'operació del sistema com a conjunt integral de components per a un fi.

c) Mesures de protecció [mp]. Se centren a protegir actius concrets, segons la seva naturalesa i la qualitat exigida pel nivell de seguretat de les dimensions afectades.

2. Selecció de mesures de seguretat

1. Per a la selecció de les mesures de seguretat se segueixen els passos següents:

a) Identificació dels tipus d'actius presents.

b) Determinació de les dimensions de seguretat rellevants, tenint en compte el que estableix l'annex I.

c) Determinació del nivell corresponent a cada dimensió de seguretat, tenint en compte el que estableix l'annex I.

d) Determinació de la categoria del sistema, segons el que estableix l'annex I.

e) Selecció de les mesures de seguretat apropiades d'entre les contingudes en aquest annex, d'acord amb les dimensions de seguretat i els seus nivells, i, per a determinades mesures de seguretat, d'acord amb la categoria del sistema.

2. A l'efecte de facilitar el compliment del que disposa aquest annex, quan en un sistema d'informació existeixin sistemes que requereixin l'aplicació d'un nivell de mesures de seguretat diferent del del sistema principal, es poden segregar d'aquest últim, i en cada cas és aplicable el nivell de mesures de seguretat corresponent i sempre que es puguin delimitar la informació i els serveis afectats.

3. La relació de mesures seleccionades s'ha de formalitzar en un document denominat declaració d'aplicabilitat, signat pel responsable de la seguretat del sistema.

4. La correspondència entre els nivells de seguretat exigits en cada dimensió i les mesures de seguretat és la que indica la taula 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	n.a.	+	++	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'incidències
T	n.a.	n.a.	aplica	op.exp.8	Registre de l'activitat dels usuaris
categoria	n.a.	aplica	=	op.exp.9	Registre de la gestió d'incidències
T	n.a.	n.a.	aplica	op.exp.10	Protecció dels registres d'activitat
categoria	aplica	=	+	op.exp.11	Protecció de claus criptogràfiques
				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.	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 enfront d'incendis
D	n.a.	aplica	=	mp.if.6	Protecció contra 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	n.a.	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
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	n.a.	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

A les taules del present annex s'utilitzen les convencions següents:

a) Per indicar que una determinada mesura de seguretat s'ha d'aplicar a una o diverses dimensions de seguretat en algun nivell determinat s'utilitza la veu «aplica».

b) «n.a.» significa «no aplica».

c) Per indicar que les exigències d'un nivell són iguals que les del nivell inferior s'utilitza el signe «=».

d) Per indicar l'increment d'exigències graduat en funció del nivell de la dimensió de seguretat, s'utilitzen els signes «+» i «++».

e) Per indicar que una mesura protegeix específicament una certa dimensió de seguretat, aquesta s'explicita mitjançant la seva inicial.

3. Marc organitzatiu [org]

El marc organitzatiu està constituït per un conjunt de mesures relacionades amb l'organització global de la seguretat.

3.1 Política de seguretat [org.1].

dimensions	Totes		
categoria	bàsica	mitjana	alta
	aplica	=	=

La política de seguretat ha de ser aprovada per l'òrgan superior competent que correspongui, d'acord amb el que estableix l'article 11, i s'ha de plasmar en un document escrit, en el qual, de forma clara, es precisi, almenys, el següent:

a) Els objectius o missió de l'organització.

b) El marc legal i regulador en el qual s'han de portar a terme les activitats.

c) Els rols o funcions de seguretat, definint per a cadascun els deures i responsabilitats del càrrec, així com el procediment per a la seva designació i renovació.

d) L'estructura del comitè o els comitès per a la gestió i coordinació de la seguretat, detallant-ne l'àmbit de responsabilitat, els membres i la relació amb altres elements de l'organització.

e) Les directrius per a l'estructuració de la documentació de seguretat del sistema, la gestió i accés.

La política de seguretat ha de referenciar el que estableix el Document de Seguretat que exigeix el Reial decret 1720/2007 i ser coherent amb aquest en el que correspongui.

3.2 Normativa de seguretat [org.2].

dimensions	Totes		
categoria	bàsica	mitjana	alta
	aplica	=	=

S'ha de disposar d'una sèrie de documents que descriguin:

a) L'ús correcte d'equips, serveis i instal·lacions.

b) El que es considera ús indegut.

c) La responsabilitat del personal respecte del compliment o violació d'aquestes normes: drets, deures i mesures disciplinàries d'acord amb la legislació vigent.

3.3 Procediments de seguretat [org.3].

dimensions	Totes		
categoria	bàsica	mitjana	alta
	aplica	=	=

S'ha de disposar d'una sèrie de documents que detallin de forma clara i precisa:

a) Com portar a terme les tasques habituals.

b) Qui ha de fer cada tasca.

c) Com identificar i reportar comportaments anòmals.

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.

4. **Marc operacional [op]**

El marc operacional està constituït per les mesures que s'han de prendre per protegir l'operació del sistema com a conjunt integral de components per a un fi.

4.1 Planificació [op.pl].

4.1.1 Anàlisi de riscos [op.pl.1].

dimensions	Totes		
categoria	bàsica	mitjana	alta
	aplica	+	++

Categoria BÀSICA

És suficient una anàlisi informal, realitzada en llenguatge natural. És a dir, una exposició textual que descrigui els aspectes següents:

a) Identifiqui els actius més valuosos del sistema.
b) Identifiqui les amenaces més probables.
c) Identifiqui les salvaguardes que protegeixen de les amenaces esmentades.
d) Identifiqui els riscos residuals principals.

Categoria MITJANA

S'ha de fer una anàlisi semiformal, utilitzant un llenguatge específic, amb un catàleg bàsic d'amenaces i una semàntica definida. És a dir, una presentació amb taules que descrigui els aspectes següents:

a) Identifiqui i valori qualitativament els actius més valuosos del sistema.
b) Identifiqui i quantifiqui les amenaces més probables.
c) Identifiqui i valori les salvaguardes que protegeixen de les amenaces.
d) Identifiqui i valori el risc residual.

Categoria ALTA

S'ha de realitzar una anàlisi formal, utilitzant un llenguatge específic, amb un fonament matemàtic reconegut internacionalment. L'anàlisi ha de cobrir els aspectes següents:

a) Identifiqui i valori qualitativament els actius més valuosos del sistema.
b) Identifiqui i quantifiqui les amenaces possibles.
c) Identifiqui les vulnerabilitats habilitadores de les amenaces.
d) Identifiqui i valori les salvaguardes adequades.
e) Identifiqui i valori el risc residual.

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 detallant, almenys, els aspectes següents:

a) Documentació de les instal·lacions:

1r Àrees.
2n Punts d'accés.

b) Documentació del sistema:

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

c) Esquema de línies de defensa:

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

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

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

e) Controls tècnics interns:

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

f) Sistema de gestió amb actualització i aprovació periòdica.

4.1.3 Adquisició de nous components [op.pl.3].

dimensions	Totes		
categoria	bàsica	mitjana	alta
	aplica	=	=

S'ha d'establir un procés formal per planificar l'adquisició de nous components del sistema, procés que:

a) Ha d'atendre les conclusions de l'anàlisi de riscos: [op.pl.1].
b) Ha de ser conforme a l'arquitectura de seguretat escollida: [op.pl.2].
c) Ha de preveure les necessitats tècniques, de formació i de finançament de forma conjunta.

4.1.4 Dimensionament / gestió de capacitats [op.pl.4].

dimensions	D		
nivell	baix	mitjà	alt
	no aplica	aplica	=

Amb caràcter previ a la posada en explotació, s'ha de realitzar un estudi previ que cobreixi els aspectes següents:

a) Necessitats de processament.
b) Necessitats d'emmagatzematge d'informació: durant el processament i durant el període que s'hagi de retenir.
d) Necessitats de comunicació.
e) Necessitats de personal: quantitat i qualificació professional.
f) Necessitats d'instal·lacions i mitjans auxiliars.

4.1.5 Components certificats [op.pl.5].

dimensions	Totes		
categoria	bàsica	mitjana	alta
	no aplica	no aplica	aplica

S'han d'utilitzar preferentment sistemes, productes o equips amb les funcionalitats de seguretat i nivell que hagin estat avaluats de conformitat amb normes europees o internacionals i que estiguin certificats per entitats independents de solvència reconeguda.

Tenen la consideració de normes europees o internacionals, ISO/IEC 15408 o altres de naturalesa i qualitat anàlogues.

Tenen la consideració d'entitats independents de reconeguda solvència les recollides en els acords o arranjaments internacionals de reconeixement mutu dels certificats de la seguretat de la tecnologia de la informació o altres de naturalesa anàloga.

4.2 Control d'accés. [op.acc].

El control d'accés cobreix el conjunt d'activitats preparatòries i executives perquè una determinada entitat, usuari o procés pugui, o no, accedir a un recurs del sistema per realitzar una acció determinada.

El control d'accés que s'implanti en un sistema real ha de ser un punt d'equilibri entre la comoditat d'ús i la protecció de la informació. En sistemes de nivell Baix, s'ha de donar prioritat a la comoditat, mentre que en sistemes de nivell Alt ha de prevaldre la protecció.

En tot control d'accés es requereix el següent:

a) Que tot accés estigui prohibit, excepte concessió expressa.
b) Que l'entitat quedi identificada singularment [op.acc.1].
c) Que la utilització dels recursos estigui protegida [op.acc.2].
d) Que es defineixin per a cada entitat els paràmetres següents: a què es necessita accedir, amb quins drets i sota quina autorització [op.acc.4].
e) Han de ser diferents les persones que autoritzen, utilitzen i controlen l'ús [op.acc.3].
f) Que la identitat de l'entitat quedi suficientment autenticada [mp.acc.5].
g) Que es controli tant l'accés local ([op.acc.6]) com l'accés remot ([op.acc.7]).

Amb el compliment de totes les mesures indicades s'ha de garantir que ningú accedeix a recursos sense autorització. A més, queda registrat l'ús del sistema ([op.exp.8]) per poder detectar qualsevol avaria accidental o deliberada i reaccionar.

Quan s'interconnectin sistemes en els quals la identificació, autenticació i autorització tinguin lloc en diferents dominis de seguretat, sota diferents responsabilitats, en els casos en què sigui necessari, les mesures de seguretat locals s'han d'acompanyar amb els acords de col·laboració corresponents que delimitin mecanismes i procediments per a l'atribució i exercici efectius de les responsabilitats de cada sistema ([op.ext]).

4.2.1 Identificació [op.acc.1].

dimensions	A T		
nivell	baix	mitjà	alt
	aplica	=	=

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

a) S'ha d'assignar un identificador singular per a cada entitat (usuari o procés) que accedeix al sistema, de tal forma que:

1r Es pot saber qui rep i quins drets d'accés rep.
2n Es pot saber qui ha fet alguna cosa i què ha fet.

b) Els comptes d'usuari s'han de gestionar de la manera següent:

1r Cada compte està associat a un identificador únic.
2n 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 la va autoritzar dóna ordre en sentit contrari.
3r 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.

4.2.2 Requisits d'accés [op.acc.2].

dimensions	I C A T		
nivell	baix	mitjà	alt
	aplica	=	=

Els requisits d'accés s'han d'atenir al que s'indica a continuació:

a) Els recursos del sistema s'han de protegir amb algun mecanisme que n'impedeixi la utilització, llevat de les entitats que gaudeixin de drets d'accés suficients.
b) Els drets d'accés de cada recurs s'han d'establir segons les decisions de la persona responsable del recurs, i s'han d'atenir a la política i la normativa de seguretat del sistema.
c) Particularment s'ha de controlar l'accés als components del sistema i als seus fitxers o registres de configuració.

4.2.3 Segregació de funcions i tasques [op.acc.3].

dimensions	I C A T		
nivell	baix	mitjà	alt
	no aplica	aplica	=

El sistema de control d'accés s'ha d'organitzar de forma que s'exigeixi la concurrència de dues o més persones per realitzar tasques crítiques, i que anul·li la possibilitat que un sol individu autoritzat pugui abusar dels seus drets per cometre alguna acció il·lícita.
En concret, s'han de separar almenys les funcions següents:

a) Desenvolupament d'operació.
b) Configuració i manteniment del sistema d'operació.
c) Auditoria o supervisió de qualsevol altra funció.

4.2.4 Procés de gestió de drets d'accés [op.acc.4].

dimensions	I C A T		
nivell	baix	mitjà	alt
	aplica	=	=

Els drets d'accés de cada usuari s'han de limitar atenent els principis següents:

a) Mínim privilegi. Els privilegis de cada usuari s'han de reduir al mínim estrictament necessari per complir les seves obligacions. D'aquesta manera es delimiten els danys que pugui causar una entitat, de forma accidental o intencionada.
b) Necessitat de conèixer. Els privilegis s'han de limitar de forma que els usuaris només accedeixin al coneixement d'aquella informació requerida per complir les seves obligacions.

c) Capacitat d'autoritzar. Només i exclusivament el personal amb competència per a això pot concedir, alterar o anul·lar l'autorització d'accés als recursos, de conformitat amb els criteris establerts pel seu propietari.

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

dimensions	I C A T		
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.

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

Nivell BAIX

a) S'admet l'ús de qualsevol mecanisme d'autenticació: claus concertades, o dispositius físics (en expressió anglesa «tokens») o components lògics com ara certificats de programari o altres d'equivalents o mecanismes biomètrics.

b) En el cas de fer servir contrasenyes s'han d'aplicar regles bàsiques de qualitat.

c) S'ha d'atendre la seguretat dels autenticadors de forma que:

1r Els autenticadors s'han d'activar una vegada estiguin sota el control efectiu de l'usuari.

2n Els autenticadors han d'estar sota el control exclusiu de l'usuari.

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

4t Els autenticadors s'han de canviar amb una periodicitat marcada per la política de l'organització, atenent la categoria del sistema al qual s'accedeix.

5è Els autenticadors s'han de retirar i ser deshabilitats quan l'entitat (persona, equip o procés) que autentiquen acaba la seva relació amb el sistema.

Nivell MITJÀ

a) No es recomana l'ús de claus concertades.

b) Es recomana l'ús d'un altre tipus de mecanismes del tipus dispositius físics («tokens») o components lògics com ara certificats de programari o altres d'equivalents o biomètrics.

c) En el cas de fer servir contrasenyes s'han d'aplicar polítiques rigoroses de qualitat de la contrasenya i renovació freqüent.

Nivell ALT

a) Els autenticadors se suspenen després d'un període definit de no ser utilitzats.

b) No s'admet l'ús de claus concertades.

c) S'exigeix l'ús de dispositius físics («tokens») personalitzats o biometria.

d) En el cas d'utilització de dispositius físics («tokens») s'han d'utilitzar algoritmes acreditats pel Centre Criptològic Nacional.

e) S'han d'utilitzar, preferentment, productes certificats [op.pl.5].

Taula resum de mecanismes d'autenticació admissibles

		Nivell		
		BAIX	MITJÀ	ALT
alguna cosa que se sap	claus concertades	sí	Amb cautela	no
alguna cosa que es té	«tokens»	si	sí	criptogràfics
alguna cosa que s'és	biometria	sí	sí	+ doble factor

4.2.6 Accés local [op.acc.6].0

dimensions	I C A T		
nivell	baix	mitjà	alt
	aplica	+	++

Es considera accés local el realitzat des de llocs de treball dins de les mateixes instal·lacions de l'organització. Aquests accessos han de tenir en compte el nivell de les dimensions de seguretat:

Nivell BAIX

a) S'han de prevenir atacs que puguin revelar informació del sistema sense arribar a accedir-hi. La informació revelada a qui intenta accedir-hi ha de ser la mínima imprescindible (els diàlegs d'accés només han de proporcionar la informació indispensable).
b) El nombre d'intents permesos ha de ser limitat, i s'ha de bloquejar l'oportunitat d'accés una vegada efectuats un cert nombre d'errors consecutius.
c) S'han de registrar els accessos amb èxit, i els fallits.
d) El sistema ha d'informar l'usuari de les seves obligacions immediatament després d'obtenir l'accés.

Nivell MITJÀ

S'ha d'informar l'usuari de l'últim accés efectuat amb la seva identitat.

Nivell ALT

a) L'accés ha d'estar limitat per horari, dates i lloc des d'on s'accedeix.
b) S'han de definir els punts en què el sistema requereix una renovació de l'autenticació de l'usuari, mitjançant identificació singular, sense que n'hi hagi prou amb la sessió establerta.

4.2.7 Accés remot [op.acc.7].

dimensions	I C A T		
nivell	baix	mitjà	alt
	aplica	+	=

Es considera accés remot el realitzat des de fora de les mateixes instal·lacions de l'organització, a través de xarxes de tercers.
S'ha de garantir la seguretat del sistema quan hi accedeixin remotament usuaris o altres entitats, cosa que implica protegir tant l'accés en si mateix (com a [op.acc.6]) com el canal d'accés remot (com a [mp.com.2] i [mp.com.3]).

Nivell MITJÀ

S'ha d'establir una política específica del que es pot fer remotament, per a la qual cosa es requereix autorització positiva.

4.3 Explotació [op.exp].

4.3.1 Inventari d'actius [op.exp.1].

dimensions	Totes		
categoria	bàsica	mitjana	alta
	aplica	=	=

S'ha de mantenir un inventari actualitzat de tots els elements del sistema, detallant-ne la naturalesa i identificant-ne el propietari; és a dir, la persona que és responsable de les decisions relatives al sistema.

4.3.2 Configuració de seguretat [op.exp.2].

dimensions	Totes		
categoria	bàsica	mitjana	alta
	aplica	=	=

S'han de configurar els equips prèviament a la seva entrada en operació, de forma que:

a) Es retirin comptes i contrasenyes estàndard.
b) S'ha d'aplicar la regla de «mínima funcionalitat»:

1r El sistema ha de proporcionar la funcionalitat requerida perquè l'organització assoleixi els seus objectius i cap altra funcionalitat.
2n No ha de proporcionar funcions gratuïtes, ni d'operació, ni d'administració, ni d'auditoria, de manera que es redueixi el seu perímetre al mínim imprescindible.
3r S'han d'eliminar o desactivar mitjançant el control de la configuració les funcions que no siguin d'interès, no siguin necessàries, i fins i tot les que siguin inadequades al fi que es persegueix.

c) S'ha d'aplicar la regla de «seguretat per defecte»:

1r Les mesures de seguretat han de ser respectuoses amb l'usuari i protegir-lo, llevat que s'exposi conscientment a un risc.
2n Per reduir la seguretat, l'usuari ha de realitzar accions conscients.
3r L'ús natural, en els casos que l'usuari no ha consultat el manual, és un ús segur.

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

dimensions	Totes		
categoria	bàsica	mitjana	alta
	no aplica	aplica	=

S'ha de gestionar de forma 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 incidències (vegeu [op.exp.7]).

4.3.4 Manteniment [op.exp.4].

dimensions	Totes		
categoria	bàsica	mitjana	alta
	aplica	=	=

Per mantenir l'equipament físic i lògic que constitueix el sistema s'ha d'aplicar el següent:

a) S'han d'atendre les especificacions dels fabricants quant a instal·lació i manteniment dels sistemes.
b) S'ha de fer un seguiment continu dels anuncis de defectes.
c) S'ha de disposar d'un procediment per analitzar, prioritzar i determinar quan aplicar les actualitzacions de seguretat, pedaços, millores i noves versions. La priorització ha de tenir en compte la variació del risc en funció de l'aplicació o no de l'actualització.

4.3.5 Gestió de canvis [op.exp.5].

dimensions	Totes		
categoria	bàsica	mitjana	alta
	no aplica	aplica	=

S'ha de mantenir un control continu de canvis realitzats en el sistema, de forma que:

a) Tots els canvis anunciats pel fabricant o proveïdor s'han d'analitzar per determinar-ne la conveniència per ser incorporats o no.
b) Abans de posar en producció una nova versió o una versió apedaçada, s'ha de comprovar en un equip que no estigui en producció que la nova instal·lació funciona correctament i no disminueix l'eficàcia de les funcions necessàries per a la feina diària. L'equip de proves ha de ser equivalent al de producció en els aspectes que es comproven.
c) Els canvis s'han de planificar per reduir l'impacte sobre la prestació dels serveis afectats.
d) Mitjançant anàlisis de riscos s'ha de determinar si els canvis són rellevants per a la seguretat del sistema. Els canvis que impliquin una situació de risc de nivell alt s'han d'aprovar explícitament de forma prèvia a la implantació.

4.3.6 Protecció contra codi perjudicial [op.exp.6].

dimensions	Totes		
categoria	bàsica	mitjana	alta
	aplica	=	=

Es consideren codi perjudicial: els virus, els cucs, els troians, els programes espies, coneguts en terminologia anglesa com a «spyware», i, en general, tot el que es coneix com a «malware».
S'ha de disposar de mecanismes de prevenció i reacció contra un codi perjudicial amb manteniment d'acord amb les recomanacions del fabricant.

4.3.7 Gestió d'incidències [op.exp.7].

dimensions	Totes		
categoria	bàsica	mitjana	alta
	no aplica	aplica	=

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'incidents reals o sospitosos, detallant l'escalat de la notificació.
b) Procediment de presa de mesures urgents, incloent-hi l'aturada de serveis, l'aïllament del sistema afectat, la recollida d'evidències i 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:

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

La gestió d'incidents que afectin dades de caràcter personal ha de tenir en compte el que disposa el Reial decret 1720/2007, en el que correspongui.

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

dimensions	T		
nivel	baix	mitjà	alt
	no aplica	no aplica	aplica

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

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

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

dimensions	Totes		
categoria	bàsica	mitjana	alta
	no aplica	aplica	=

S'han de registrar totes les actuacions relacionades amb la gestió d'incidències, de forma 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, posteriorment, sustentar 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 de les incidències, s'ha de revisar la determinació dels esdeveniments auditables.

4.3.10 Protecció dels registres d'activitat [op.exp.10].

dimensions	T		
nivel	baix	mitjà	alt
	no aplica	no aplica	aplica

S'han de protegir els registres del sistema, de forma que:

a) S'ha de determinar el període de retenció dels registres.
b) S'ha d'assegurar la data i hora. Vegeu [mp.info.5].
c) Els registres no poden ser modificats ni eliminats per personal no autoritzat.
d) Les còpies de seguretat, si n'hi ha, s'han d'ajustar als mateixos requisits.

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 de fer servir programes avaluats o dispositius criptogràfics certificats.
b) S'han d'utilitzar algoritmes acreditats pel Centre Criptològic Nacional.

4.4 Serveis externs [op.ext].

Quan s'utilitzin recursos externs a l'organització, siguin serveis, equips, instal·lacions o personal, s'ha de tenir en compte que la delegació es limita a les funcions.

L'organització segueix sent en tot moment responsable dels riscos en què s'incorre en la mesura que impactin sobre la informació manejada i els serveis finals prestats per l'organització.

L'organització ha de disposar les mesures necessàries per poder exercir la seva responsabilitat i mantenir el control en tot moment.

4.4.1 Contractació i acords de nivell de servei [op.ext.1].

dimensions	Totes		
categoria	bàsica	mitjana	alta
	no aplica	aplica	=

Prèviament a la utilització de recursos externs s'han d'establir contractualment les característiques del servei prestat i les responsabilitats de les parts. S'ha de detallar el que es considera qualitat mínima del servei prestat i les conseqüències del seu incompliment.

4.4.2 Gestió diària [op.ext.2].

dimensions	Totes		
categoria	bàsica	mitjana	alta
	no aplica	aplica	=

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'incidències i desastres (vegeu [op.exp.7]).

4.4.3 Mitjans alternatius [op.ext.9].

dimensions	D		
nivel	baix	mitjà	alt
	no aplica	no aplica	aplica

Ha d'estar prevista la provisió del servei per mitjans alternatius en cas d'indisponibilitat del servei contractat. El servei alternatiu ha de tenir les mateixes garanties de seguretat que el servei habitual.

4.5 Continuïtat del servei [op.cont].

4.5.1 Anàlisi d'impacte [op.cont.1].

dimensions	D		
nivel	baix	mitjà	alt
	no aplica	aplica	=

S'ha de dur a terme una anàlisi d'impacte que permeti determinar:

a) Els requisits de disponibilitat de cada servei mesurats com l'impacte d'una interrupció durant un cert període de temps.
b) Els elements que són crítics per a la prestació de cada servei.

4.5.2 Pla de continuïtat [op.cont.2].

dimensions	D		
nivel	baix	mitjà	alt
	no aplica	no aplica	aplica

S'ha de desenvolupar un pla de continuïtat que estableixi les accions a executar en cas d'interrupció dels serveis prestats amb els mitjans habituals. Aquest pla ha de preveure els aspectes següents:

a) S'han d'identificar funcions, responsabilitats i activitats a realitzar.
b) Hi ha d'haver una previsió dels mitjans alternatius que es conjugaran per poder seguir prestant els serveis.
c) Tots els mitjans alternatius han d'estar planificats i materialitzats en acords o contractes amb els proveïdors corresponents.
d) Les persones afectades pel pla han de rebre formació específica relativa al seu paper en l'esmentat pla.
e) El pla de continuïtat ha de ser part integral i harmònica dels plans de continuïtat de l'organització en altres matèries alienes a la seguretat.

4.5.3 Proves periòdiques [op.cont.3].

dimensions	D		
nivel	baix	mitjà	alt
	no aplica	no aplica	aplica

S'han de fer proves periòdiques per localitzar, i corregir si s'escau, els errors o deficiències que hi pugui haver en el pla de continuïtat.

4.6 Monitorització del sistema [op.mon].

El sistema ha d'estar subjecte a mesures de monitorització de la seva activitat.

4.6.1 Detecció d'intrusió [op.mon.1].

dimensions	Totes		
categoria	bàsica	mitjana	alta
	no aplica	no aplica	aplica

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
	no aplica	no aplica	aplica

S'ha d'establir un conjunt d'indicadors que mesuri el desenvolupament real del sistema en matèria de seguretat, en els aspectes següents:

a) Grau d'implantació de les mesures de seguretat.
b) Eficàcia i eficiència de les mesures de seguretat.
c) Impacte dels incidents de seguretat.

5. **Mesures de protecció [mp]**

Les mesures de protecció s'han de centrar a protegir actius concrets, segons la seva naturalesa, amb el nivell requerit en cada dimensió de seguretat.

5.1 Protecció de les instal·lacions i infraestructures [mp.if].

5.1.1 Àrees separades i amb control d'accés [mp.if.1].

dimensions	totes		
categoria	bàsica	mitjana	alta
	aplica	=	=

L'equipament s'ha d'instal·lar en àrees separades específiques per a la seva funció.
S'han de controlar els accessos a les àrees indicades de manera que només s'hi pugui accedir per les entrades previstes i vigilades.

5.1.2 Identificació de les persones [mp.if.2].

dimensions	totes		
categoria	bàsica	mitjana	alta
	aplica	=	=

El mecanisme de control d'accés s'ha d'atenir al que es disposa a continuació:

a) S'han d'identificar totes les persones que accedeixin als locals on hi ha equipament que formi part del sistema d'informació.
b) S'han de registrar les entrades i sortides de persones.

5.1.3 Condicionament dels locals [mp.if.3].

dimensions	totes		
categoria	bàsica	mitjana	alta
	aplica	=	=

Els locals on s'ubiquin els sistemes d'informació i els seus components han de disposar d'elements adequats per al funcionament eficaç de l'equipament instal·lat allà. I, especialment:

a) Condicions de temperatura i humitat.
b) Protecció contra les amenaces identificades en l'anàlisi de riscos.
c) Protecció del cablatge contra incidents fortuïts o deliberats.

5.1.4 Energia elèctrica [mp.if.4].

dimensions	D		
nivell	baix	mitjà	alt
	aplica	+	=

Els locals on s'ubiquin els sistemes d'informació i els seus components han de disposar de l'energia elèctrica, i les seves preses corresponents, necessària per funcionar, de forma que en els dits locals:

a) Es garanteixi el subministrament de potència elèctrica.
b) Es garanteixi el funcionament correcte dels llums d'emergència.

Nivell MITJÀ

S'ha de garantir el subministrament elèctric als sistemes en cas de fallada del subministrament general, i garantir el temps suficient perquè finalitzin ordenadament els processos, salvaguardant la informació.

5.1.5 Protecció contra incendis [mp.if.5].

dimensions	D		
nivell	baix	mitjà	alt
	aplica	=	=

Els locals on s'ubiquin els sistemes d'informació i els seus components s'han de protegir contra incendis fortuïts o deliberats, aplicant almenys la normativa industrial pertinent.

5.1.6 Protecció contra inundacions [mp.if.6].

dimensions	D		
nivell	baix	mitjà	alt
	no aplica	aplica	=

Els locals on s'ubiquin els sistemes d'informació i els seus components s'han de protegir contra incidents fortuïts o deliberats causats per l'aigua.

5.1.7 Registre d'entrada i sortida d'equipament [mp.if.7].

dimensions	totes		
categoria	baix	mitjà	alt
	aplica	=	=

S'ha de portar un registre detallat de qualsevol entrada i sortida d'equipament, incloent-hi la identificació de la persona que autoritza el moviment.

5.1.8 Instal·lacions alternatives [mp.if.9].

dimensions	D		
nivell	baix	mitjà	alt
	no aplica	no aplica	aplica

S'ha de garantir l'existència i disponibilitat d'instal·lacions alternatives per poder treballar en cas que les instal·lacions habituals no estiguin disponibles. Les instal·lacions alternatives han de tenir les mateixes garanties de seguretat que les instal·lacions habituals.

5.2 Gestió del personal [mp.per].

5.2.1 Caracterització del lloc de treball [mp.per.1].

dimensions	totes		
categoria	baix	mitjà	alt
	no aplica	aplica	=

Cada lloc de treball s'ha de caracteritzar de la manera següent:

a) S'han de definir les responsabilitats relacionades amb cada lloc de treball en matèria de seguretat. La definició s'ha de basar en l'anàlisi de riscos.
b) S'han de definir els requisits que han de satisfer les persones que ocuparan el lloc de treball, en particular, en termes de confidencialitat.
c) Aquests requisits s'han de tenir en compte en la selecció de la persona que ocuparà el lloc, incloent-hi la verificació dels seus antecedents laborals, formació i altres referències.

5.2.2 Deures i obligacions [mp.per.2].

dimensions	totes		
categoria	bàsica	mitjana	alta
	aplica	=	=

1. S'ha d'informar cada persona que treballi en el sistema dels deures i responsabilitats del seu lloc de treball en matèria de seguretat.

a) S'han d'especificar les mesures disciplinàries que siguin procedents.
b) S'ha de cobrir tant el període durant el qual s'exerceix el lloc com les obligacions en cas de finalització de l'assignació, o trasllat a un altre lloc de treball.
c) S'ha de preveure el deure de confidencialitat respecte de les dades a què tingui accés, tant durant el període que estigui adscrit al lloc de treball com posteriorment a la finalització.

2. En cas de personal contractat a través d'un tercer:

a) S'han d'establir els deures i obligacions del personal.
b) S'han d'establir els deures i obligacions de cada part.
c) S'ha d'establir el procediment de resolució d'incidents relacionats amb l'incompliment de les obligacions.

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 quant al 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 hagin de ser reportats per al seu tractament per personal especialitzat.
c) El procediment de report d'incidències de seguretat, siguin reals o falses alarmes.

5.2.4 Formació [mp.per.4].

dimensions	totes		
categoria	bàsica	mitjana	alta
	aplica	=	=

S'ha de formar regularment el personal en les matèries que siguin necessàries per a l'exercici de les seves funcions, en particular pel que fa a:

a) Configuració de sistemes.
b) Detecció i reacció a incidents.
c) Gestió de la informació en qualsevol suport en què es trobi. S'han de cobrir almenys les activitats següents: emmagatzematge, transferència, còpies, distribució i destrucció.

5.2.5 Personal alternatiu [mp.per.9].

dimensions	D		
nivell	baix	mitjà	alt
	no aplica	no aplica	aplica

S'ha de garantir l'existència i disponibilitat d'altres persones que es puguin fer càrrec de les funcions en cas d'indisponibilitat del personal habitual. El personal alternatiu ha d'estar sotmès a les mateixes garanties de seguretat que el personal habitual.

5.3 Protecció dels equips [mp.eq].

5.3.1 Lloc de treball endreçat [mp.eq.1].

dimensions	totes		
categoria	bàsica	mitjana	alta
	aplica	+	=

S'ha d'exigir que els llocs de treball estiguin endreçats, sense més material damunt la taula que el requerit per a l'activitat que es realitza en cada moment.

Categoria MITJANA

Aquest material s'ha de guardar en un lloc tancat quan no s'utilitzi.

5.3.2 Bloqueig de lloc de treball [mp.eq.2].

dimensions	A		
nivell	baix	mitjà	alt
	no aplica	aplica	+

El lloc de treball s'ha de bloquejar al cap d'un temps prudencial d'inactivitat i ha de requerir una nova autenticació de l'usuari per reprendre l'activitat en curs.

Categoria ALTA

Passat un cert temps, superior a l'anterior, s'han de cancel·lar les sessions obertes des de l'esmentat lloc de treball.

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

dimensions	totes		
categoria	bàsica	mitjana	alta
	aplica	=	+

Els equips que abandonin 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 responsable de l'equip i un control regular conforme està positivament sota el seu control.

b) S'ha d'establir un canal de comunicació per informar de pèrdues o sostraccions el servei de gestió d'incidències.

c) S'ha d'establir un sistema de protecció perimetral que minimitzi la visibilitat exterior i controli les opcions d'accés a l'interior quan l'equip es connecti a xarxes, en particular si l'equip es connecta a xarxes públiques.

d) S'ha d'evitar, en la mesura que sigui possible, que l'equip contingui claus d'accés remot a l'organització. Es consideren claus d'accés les que són 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 al disc s'ha de protegir mitjançant xifratge.

5.3.4 Mitjans alternatius [mp.eq.9].

dimensions	D		
nivell	baix	mitjà	alt
	No aplica	aplica	=

S'ha de garantir l'existència i disponibilitat de mitjans alternatius de tractament de la informació per al cas que fallin els mitjans habituals. Aquests mitjans alternatius han d'estar subjectes a les mateixes garanties de protecció.

Igualment, s'ha d'establir un temps màxim perquè els equips alternatius entrin en funcionament.

5.4 Protecció de les comunicacions [mp.com].

5.4.1 Perímetre segur [mp.com.1].

dimensions	totes		
categoria	bàsica	mitjana	alta
	aplica	=	+

S'ha de disposar un sistema tallafocs que separi la xarxa interna de l'exterior. Tot el trànsit ha de travessar aquest tallafocs, que només ha de deixar transitar els fluxos prèviament autoritzats.

Categoria ALTA

a) El sistema de tallafocs ha de constar de dos o més equips de diferent fabricant disposats en cascada.

b) S'han de disposar sistemes redundants.

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 maquinari en l'establiment i la utilització de la xarxa privada virtual.
b) S'han d'utilitzar, preferentment, productes certificats [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 cap informació (vegeu [op.acc.5]).
b) S'han de prevenir atacs actius, garantint que almenys seran detectats, i s'han d'activar els procediments previstos de tractament de l'incident. Es consideren atacs actius:

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

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'ha de valorar positivament l'ús de dispositius maquinari en l'establiment i la utilització de la xarxa privada virtual.
b) S'han d'utilitzar, preferentment, productes certificats [op.pl.5].

5.4.4 Segregació de xarxes [mp.com.4].

dimensions	totes		
categoria	bàsica	mitjana	alta
	no aplica	no aplica	aplica

La segregació de xarxes delimita l'accés a la informació i, conseqüentment, la propagació dels incidents de seguretat, que queden restringits a l'entorn on passen.

La xarxa s'ha de segmentar en segments de forma que hi hagi:

a) Control d'entrada dels usuaris que arriben a cada segment.

b) Control de sortida de la informació disponible en cada segment.

c) Les xarxes es poden segmentar per dispositius físics o lògics. El punt d'interconnexió ha d'estar particularment assegurat, mantingut i monitorat (com a [mp.com.1]).

5.4.5 Mitjans alternatius [mp.com.9].

dimensions	D		
nivell	baix	mitjà	alt
	no aplica	no aplica	aplica

S'ha de garantir l'existència i disponibilitat de mitjans alternatius de comunicació per al cas que fallin els mitjans habituals. Els mitjans alternatius de comunicació:

a) Han d'estar subjectes i proporcionar les mateixes garanties de protecció que el mitjà habitual.

b) Han de garantir un temps màxim d'entrada en funcionament.

5.5 Protecció dels suports d'informació [mp.si].

5.5.1 Etiquetatge [mp.si.1].

dimensions	C		
nivell	baix	mitjà	alt
	aplica	=	=

Els suports d'informació s'han d'etiquetar de forma que, sense revelar el seu contingut, s'indiqui el nivell de seguretat de la informació continguda de més qualificació.

Els usuaris han d'estar capacitats per entendre el significat de les etiquetes, o bé mitjançant simple inspecció, o bé mitjançant el recurs a un repositori que l'expliqui.

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.

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, preferentment, productes certificats [op.pl.5].

5.5.3 Custòdia [mp.si.3].

dimensions	totes		
categoria	bàsica	mitjana	alta
	aplica	=	=

S'ha d'aplicar la deguda diligència i control als suports d'informació que estan sota la responsabilitat de l'organització, mitjançant les actuacions següents:

a) Garantint el control d'accés amb mesures físiques ([mp.if.1] i [mpl.if.7]) o lògiques ([mp.si.2]), o totes dues.
b) Garantint que es respecten les exigències de manteniment del fabricant, especialment, quant a temperatura, humitat i altres agressors mediambientals.

5.5.4 Transport [mp.si.4].

dimensions	totes		
categoria	bàsica	mitjana	alta
	aplica	=	=

El responsable de sistemes ha de garantir que els dispositius estan sota control i que satisfan els seus requisits de seguretat mentre estan sent desplaçats d'un lloc a un altre.
A aquest efecte:

a) S'ha de disposar d'un registre de sortida que identifiqui el transportista que rep el suport per traslladar-lo.
b) S'ha de disposar d'un registre d'entrada que identifiqui el transportista que el lliura.
c) S'ha de disposar d'un procediment rutinari que compari les sortides amb les arribades i dispari les alarmes pertinents quan es detecti algun incident.
d) S'han d'utilitzar els mitjans de protecció criptogràfica ([mp.si.2]) corresponents al nivell de qualificació de la informació continguda de més nivell.
e) S'han de gestionar les claus segons [op.exp.11].

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

dimensions	C		
nivell	baix	mitjà	alt
	no aplica	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.

a) Els suports que s'han de reutilitzar per a una altra informació o alliberar a una altra organització han de ser objecte d'un esborrament segur del contingut anterior.
b) S'han de destruir de forma segura els suports, en els casos següents:

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

c) S'han d'utilitzar, preferentment, productes certificats [op.pl.5].

5.6 Protecció de les aplicacions informàtiques [mp.sw].

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

dimensions	totes		
categoria	bàsica	mitjana	alta
	no aplica	aplica	=

a) El desenvolupament d'aplicacions s'ha de fer sobre un sistema diferent i separat del de producció, i no han d'existir 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 emprades en proves.
3r Permeti la inspecció del codi font.

c) Els següents elements 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 tractament de pistes d'auditoria.

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

5.6.2 Acceptació i posada en servei [mp.sw.2].

dimensions	todas		
categoria	bàsica	mitjana	alta
	aplica	+	++

Categoria BÀSICA

Abans de passar a producció s'ha de comprovar el funcionament correcte de l'aplicació.

a) S'ha de comprovar que:

1r Es compleixen els criteris d'acceptació en matèria de seguretat.
2n No es deteriora la seguretat d'altres components del servei.

b) Les proves s'han de fer en un entorn aïllat (preproducció).
c) Les proves d'acceptació no s'han de fer amb dades reals, llevat que s'asseguri el nivell de seguretat corresponent.

Categoria MITJANA

S'han de fer les següents inspeccions prèvies a l'entrada en servei:

a) Anàlisis de vulnerabilitats.
b) Proves de penetració.

Categoria ALTA

S'han de fer les següents inspeccions prèvies a l'entrada en servei:

a) Anàlisis de coherència en la integració en els processos.
b) S'ha de considerar l'oportunitat de realitzar una auditoria de codi font.

5.7 Protecció de la informació [mp.info].

5.7.1 Dades de caràcter personal [mp.info.1].

dimensions	totes		
categoria	bàsica	mitjana	alta
	aplica	aplica	aplica

Quan el sistema tracti dades de caràcter personal, cal atenir-se al que disposa la Llei orgànica 15/1999, de 13 de desembre, i normes de desplegament, sense perjudici de complir, a més, les mesures que estableix aquest Reial decret.

El que indica el paràgraf anterior també s'aplica quan una disposició amb rang de llei es remeti a les normes sobre dades de caràcter personal en la protecció d'informació.

5.7.2 Qualificació de la informació [mp.info.2].

dimensions	C		
nivell	baix	mitjà	alt
	aplica	+	=

1. Per qualificar la informació cal atenir-se al que està establert legalment sobre la naturalesa de la informació.
2. La política de seguretat ha d'establir qui és el responsable de cada informació manejada pel sistema.
3. La política de seguretat ha de recollir, directament o indirectament, els criteris que, en cada organització, determinen el nivell de seguretat requerit, dins el marc establert a l'article 43 i els criteris generals prescrits a l'annex I.
4. El responsable de cada informació ha de seguir els criteris determinats a l'apartat anterior per assignar a cada informació el nivell de seguretat requerit, i és responsable de la seva documentació i aprovació formal.
5. El responsable de cada informació en cada moment té en exclusiva la potestat de modificar el nivell de seguretat requerit, d'acord amb els apartats anteriors.

Nivell MITJÀ

S'han de redactar els procediments necessaris que descriguin, amb detall, la forma en què s'ha d'etiquetar i tractar la informació en consideració al nivell de seguretat que requereix, i precisar com s'ha de fer:

a) El control d'accés.
b) L'emmagatzematge.
c) La realització de còpies.
d) L'etiquetatge de suports.
e) La transmissió telemàtica.
f) I qualsevol altra activitat relacionada amb aquesta informació.

5.7.3 Xifratge de la informació [mp.info.3].

dimensions	C		
nivell	baix	mitjà	alt
	no aplica	no aplica	aplica

Per al xifratge d'informació cal atenir-se al que s'indica a continuació:

a) La informació amb un nivell alt en confidencialitat s'ha de xifrar tant durant l'emmagatzematge com durant la transmissió. Només pot estar en clar mentre se n'està fent ús.
b) Per a l'ús de criptografia en les comunicacions, cal atenir-se al que disposa [mp.com.2].
c) Per a l'ús de criptografia en els suports d'informació, cal atenir-se al que disposa [mp.si.2].

5.7.4 Signatura electrònica [mp.info.4].

dimensions	I A		
nivell	baix	mitjà	alt
	aplica	+	++

La signatura electrònica és un mecanisme de prevenció de la repudiació; és a dir, prevé contra la possibilitat que en el futur el signatari es pugui desdir de la informació signada.
La signatura electrònica garanteix l'autenticitat del signatari i la integritat del contingut.
Quan s'utilitzi signatura electrònica:

a) El signatari és la part que es fa responsable de la informació, en la mesura de les seves atribucions.
b) S'ha de disposar d'una política de signatura electrònica, aprovada per l'òrgan superior competent que correspongui.

Nivell BAIX

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

Nivell MITJÀ

1. Els mitjans utilitzats en la signatura electrònica han de ser proporcionats a la qualificació de la informació tractada. En tot cas:

a) S'han d'utilitzar algoritmes acreditats pel Centre Criptològic Nacional.
b) S'han d'utilitzar, preferentment, certificats reconeguts.
c) S'han d'utilitzar, preferentment, dispositius segurs de signatura.

2. 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 aquest fi:

a) S'ha d'adjuntar a la signatura, o s'ha de referenciar, tota la informació pertinent per a la seva verificació i validació:

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

b) S'han de protegir la signatura i la informació esmentada a l'apartat anterior amb un segell de temps.
c) L'organisme que reculli documents signats per l'administrat ha de verificar i validar la signatura rebuda en el moment de la recepció adjuntant o referenciant sense ambigüitat la informació descrita en els epígrafs a) i b).
d) La signatura electrònica de documents per part de l'Administració ha de dur annexa o referenciada sense ambigüitat la informació descrita en els epígrafs a) i b).

Nivell ALT

S'han d'aplicar les mesures de seguretat referents a signatura electrònica exigibles en el nivell mitjà, a més de les següents:

a) S'han de fer servir certificats reconeguts.
b) S'han de fer servir dispositius segurs de creació de signatura.
c) S'han d'utilitzar, preferentment, productes certificats [op.pl.5].

5.7.5 Segells de temps [mp.info.5].

dimensions	T		
nivell	baix	mitjà	alt
	no aplica	no aplica	aplica

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].

5.7.6 Neteja de documents [mp.info.6].

dimensions	C		
nivell	baix	mitjà	alt
	aplica	=	=

En el procés de neteja de documents, se n'ha d'enretirar tota la informació addicional continguda en camps ocults, metadades, comentaris o revisions anteriors, excepte quan aquesta informació sigui pertinent per al receptor del document.
Aquesta mesura és especialment rellevant quan el document es difon àmpliament, com passa quan s'ofereix al públic en un servidor web o un altre tipus de repositori d'informació.
Cal tenir present que l'incompliment d'aquesta mesura pot perjudicar:

a) El manteniment de la confidencialitat d'informació que no s'hauria d'haver revelat al receptor del document.
b) El manteniment de la confidencialitat de les fonts o orígens de la informació, que no ha de conèixer el receptor del document.
c) La bona imatge de l'organització que difon el document ja que demostra descurança en el seu bon fer.

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

dimensions	D		
nivell	baix	mitjà	alt
	no aplica	aplica	=

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

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

Les còpies de seguretat han d'incloure:

a) Informació de treball de l'organització.
b) Aplicacions en explotació, inclosos els sistemes operatius.
c) Dades de configuració, serveis, aplicacions, equips, o altres de naturalesa anàloga.
d) Claus utilitzades per preservar la confidencialitat de la informació.

5.8 Protecció dels serveis [mp.s].

5.8.1 Protecció del correu electrònic (correu electrònic) [mp.s.1].

dimensions	totes		
categoria	básica	mitjana	alt
	aplica	=	=

El correu electrònic s'ha de protegir contra les amenaces que li són pròpies, actuant de la manera següent:

a) La informació distribuïda per mitjà de correu electrònic s'ha de protegir, tant en el cos dels missatges com en els annexos.
b) S'ha de protegir la informació d'encaminament de missatges i establiment de connexions.
c) S'ha de protegir l'organització contra els problemes que es materialitzen per mitjà del correu electrònic, en concret:

1r Correu no sol·licitat, en l'expressió anglesa «spam».
2n Programes perjudicials, constituïts per virus, cucs, troians, espies, o altres de naturalesa anàloga.
3r Codi mòbil de tipus «applet».

d) S'han d'establir normes d'ús del correu electrònic per part del personal determinat. Aquestes normes d'ús han de contenir:

1r Limitacions a l'ús com a suport de comunicacions privades.
2n Activitats de conscienciació i formació relatives a l'ús del correu electrònic.

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

dimensions	totes		
categoria	bàsica	mitjana	alt
	aplica	=	=

Els subsistemes dedicats a la publicació d'informació han de ser protegits contra 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 «cros site scripting».
d) S'han de prevenir atacs de manipulació de programes o dispositius que realitzen 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».

5.8.3 Protecció contra la denegació de servei [mp.s.8].

dimensions	D		
nivell	baix	mitjà	alt
	No aplica	aplica	+

Nivell MITJÀ

S'han d'establir mesures preventives i reactives contra atacs de denegació de servei (DOS Denial of Service). Per a això:

a) S'ha de planificar i dotar el sistema de prou capacitat per atendre la càrrega prevista amb comoditat.
b) S'han de desplegar tecnologies per prevenir els atacs coneguts.

Nivell ALT

a) S'ha d'establir un sistema de detecció d'atacs de denegació de servei.
b) S'han d'establir procediments de reacció als atacs, inclosa la comunicació amb el proveïdor de comunicacions.
c) S'ha d'impedir el llançament d'atacs des de les pròpies instal·lacions que perjudiquin tercers.

5.8.4 Mitjans alternatius [mp.s.9].

dimensions	D		
nivell	baix	mitjà	alt
	no aplica	no aplica	aplica

S'ha de garantir l'existència i disponibilitat de mitjans alternatius per prestar els serveis en cas que fallin els mitjans habituals. Aquests mitjans alternatius han d'estar subjectes a les mateixes garanties de protecció que els mitjans habituals.

6. **Desenvolupament i complement de les mesures de seguretat**

Les mesures de seguretat s'han de desenvolupar i complementar segons el que estableix la disposició final segona.

7. **Interpretació**

La interpretació del present annex cal fer-la segons el sentit propi de les seves paraules, en relació amb el context, antecedents històrics i legislatius, entre els quals figura el que disposen les instruccions tècniques CCN-STIC corresponents a la implementació i a diversos escenaris d'aplicació com ara seus electròniques, serveis de validació de certificats electrònics, serveis de datació electrònica i validació de documents datats, atenent l'esperit i les finalitat d'aquelles.

ANNEX III

Auditoria de la seguretat

1. *Objecte de l'auditoria*

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 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 realitzat una anàlisi de riscos, amb revisió i aprovació anual.
e) Que es compleixen les recomanacions de protecció descrites a l'annex II, sobre mesures de seguretat, en funció de les condicions d'aplicació 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.

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

a) Documentació dels procediments.
b) Registre d'incidències.
c) Examen del personal afectat: coneixement i praxi de les mesures que l'afecten.

2. *Nivells d'auditoria*

Els nivells d'auditoria que es realitzen als sistemes d'informació són els següents:

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 sustenten 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. 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 suggerir les possibles mesures correctores o complementàries que siguin necessàries, així com les recomanacions que es considerin oportunes. També ha d'incloure els criteris metodològics d'auditoria utilitzats, l'abast i l'objectiu de l'auditoria, i les dades, fets i 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 cal fer-la 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.

ANNEX IV

Glossari

Actiu. Component o funcionalitat d'un sistema d'informació susceptible de ser atacat de manera deliberada o accidental amb conseqüències per a l'organització. Inclou: informació, dades, serveis, aplicacions (programari), equips (maquinari), comunicacions, recursos administratius, recursos físics i recursos humans.

Anàlisi de riscos. Utilització sistemàtica de la informació disponible per identificar perills i estimar els riscos.

Auditoria de la seguretat. Revisió i examen independents dels registres i activitats del sistema per verificar la idoneïtat dels controls del sistema, assegurar que es compleixen la política de seguretat i els procediments operatius establerts, detectar les infraccions de la seguretat i recomanar modificacions apropiades dels controls, de la política i dels procediments.

Autenticitat. Propietat o característica consistent en el fet que una entitat és qui diu que és o bé que garanteix la font de la qual procedeixen les dades.

Categoria d'un sistema. És un nivell, dins de l'escala bàsica-mitjana-alta, amb què s'adjectiva un sistema a fi de seleccionar les mesures de seguretat necessàries per a aquest. La categoria del sistema recull la visió holística del conjunt d'actius com un tot harmònic, orientat a la prestació d'uns serveis.

Confidencialitat. Propietat o característica consistent en el fet que la informació ni es posa a disposició, ni es revela a individus, entitats o processos no autoritzats.

Disponibilitat. Propietat o característica dels actius consistent en el fet que les entitats o processos autoritzats hi tenen accés quan ho requereixen.

Signatura electrònica. Conjunt de dades en forma electrònica, consignades juntament a altres o associades amb aquestes, que es poden utilitzar com a mitjà d'identificació del signant.

Gestió d'incidents. Pla d'acció per atendre les incidències que es donin. A més de resoldre-les 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.

Gestió de riscos. Activitats coordinades per dirigir i controlar una organització respecte als riscos.

Incident de seguretat. Esdeveniment inesperat o no desitjat amb conseqüències en detriment de la seguretat del sistema d'informació.

Integritat. Propietat o característica consistent en el fet que l'actiu d'informació no ha estat alterat de manera no autoritzada.

Mesures de seguretat. Conjunt de disposicions encaminades a protegir-se dels riscos possibles sobre el sistema d'informació, amb la finalitat d'assegurar els seus objectius de seguretat. Es pot tractar de mesures de prevenció, de dissuasió, de protecció, de detecció i reacció, o de recuperació.

Política de signatura electrònica. Conjunt de normes de seguretat, d'organització, tècniques i legals per determinar com es generen, verifiquen i gestionen signatures electròniques, incloent-hi les característiques exigibles als certificats de signatura.

Política de seguretat. Conjunt de directrius plasmades en un document escrit, que regeixen la manera com una organització gestiona i protegeix la informació i els serveis que considera crítics.

Principis bàsics de seguretat. Fonaments que han de regir tota acció orientada a assegurar la informació i els serveis.

Procés. Conjunt organitzat d'activitats que es porten a terme per produir un producte o servei; té un principi i fi delimitats, implica recursos i dóna lloc a un resultat.

Procés de seguretat. Mètode que se segueix per assolir els objectius de seguretat de l'organització. El procés es dissenya per identificar, mesurar, gestionar i mantenir sota control els riscos a què s'enfronta el sistema en matèria de seguretat.

Requisits mínims de seguretat. Exigències necessàries per assegurar la informació i els serveis.

Risc. Estimació del grau d'exposició que una amenaça es materialitzi sobre un o més actius i causi danys o perjudicis a l'organització.

Seguretat de les xarxes i de la informació. Capacitat de les xarxes o dels sistemes d'informació de resistir, amb un determinat nivell de confiança, els accidents o accions il·lícites o malintencionades que comprometin la disponibilitat, autenticitat, integritat i confidencialitat de les dades emmagatzemades o transmeses i dels serveis que les xarxes i sistemes esmentats ofereixen o fan accessibles.

Serveis acreditats. Serveis prestats per un sistema amb autorització concedida per l'autoritat responsable, per tractar un tipus d'informació determinada, en unes condicions precises de les dimensions de seguretat, d'acord amb el seu concepte d'operació.

Sistema de gestió de la seguretat de la informació (SGSI). Sistema de gestió que, basat en l'estudi dels riscos, s'estableix per crear, implementar, fer funcionar, supervisar, revisar, mantenir 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 pugui recollir, emmagatzemar, processar o tractar, mantenir, utilitzar, compartir, distribuir, posar a disposició, presentar o transmetre.

Traçabilitat. Propietat o característica consistent en el fet que les actuacions d'una entitat poden ser imputades exclusivament a aquesta entitat.

Vulnerabilitat. Una debilitat que pot ser aprofitada per una amenaça.

Acrònims

CCN: Centre Criptològic Nacional.
CERT: Computer Emergency Reaction Team.
INTECO: Institut Nacional de Tecnologies de la Comunicació.
STIC: Seguretat de les Tecnologies d'Informació i Comunicacions.

ANNEX V

Model de clàusula administrativa particular

«Clàusula administrativa particular.–En compliment del que disposen l'article 99.4 de la Llei 30/2007, de 30 d'octubre, de contractes del sector públic, i l'article 18 del Reial decret ……/……, de …… de ……, pel qual es regula l'Esquema Nacional de Seguretat, el licitador ha d'incloure una referència precisa, documentada i acreditativa del fet que els productes de seguretat, equips, sistemes, aplicacions o els seus components han estat prèviament certificats per l'Organisme de Certificació de l'Esquema Nacional d'Avaluació i Certificació de Seguretat de les Tecnologies de la Informació.

En cas que no existeixi la certificació indicada en el paràgraf anterior, o estigui en procés, s'ha d'incloure igualment una referència precisa, documentada i acreditativa del fet que són els més idonis.

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.»