Diputació de València | Protecció de Dades i Seguretat de la Informació

CLASSIFICACIÓ: **NIVELL "A"**

(Artícle 43.1 Reglament de Política de Seguretat i de la Protecció de Dades de Carácter Personal en la Diputació Provincial de València)

NORMES DE SEGURETAT PER AL PERSONAL TÈCNIC DELS SISTEMES D'INFORMACIÓ TIC

CODI	N/SEG/TEC	**APROVACIÓ**	Decret nº 967, de 18 de gener de 2023, del President de la Diputació de València

CONTROL DOCUMENTAL

ELABORAT PER:	SUPERVISAT PER:	APROVAT PER:
	Eusebio Moya López	Antoni Francesc Gaspar
Departament de Protecció de Dades i Seguretat de la Informació	Cap Departament de Protecció de Dades i Seguretat de la Informació	President Diputació de València

HISTÓRIC DEL DOCUMENT:

Data	Edició	Revisió	Canvis Realitzats
18/01/2023	01	01	Aprovació inicial de la norma

FITXERS: NORMATIVA SEGURETAT ***LOCALITZACIÓ:***

DATA D'EMISSIÓ: Gener 2023

ÍNDEX

INTRODUCCIÓ

L'article 43.1 del Reglament pel qual es regula la política de seguretat i de la protecció de dades de caràcter personal en la Diputació Provincial de València, estableix que s'haurà d'elaborar un conjunt de regles i directrius de caràcter obligatori que desenvolupen directament el contingut de la citada política o que traslladen a l'ordre intern, mitjançant les normes corresponents, el compliment de la normativa legal aplicable en la matèria.

Aquest precepte recull expressament com integrada en el seu mandat la denominada Normativa de Seguretat, i l'article 44.1 atorga la competència per a la seua aprovació al president de la Diputació o diputat/ada en qui aquest delegue.

Per Decret num 967, de 18 de gener de 2023, el president de la Diputació de València ha aprovat les presents Normes de Seguretat per al Personal Tècnic dels Sistemes d'Informació TIC.

En el present document consta la normativa interna relacionada amb la seguretat dels sistemes d'informació TIC de la Diputació de València que han de complir els tècnics d'aquests sistemes d'informació. D'acord amb l'article 4 del citat Reglament de política de seguretat i de la protecció de dades de caràcter personal, la present normativa és aplicable als departaments en què s'integre el personal tècnic dels sistemes d'informació TIC, i resultarà d'obligat compliment per a tot el personal tècnic citat.

1. CONCEPTES BÀSICS. DEFINICIONS

Als efectes previstos en aquesta normativa, les definicions, paraules, expressions i termes s'han d'entendre en el sentit indicat en el Reglament pel qual es regula la política de seguretat i de la protecció de dades de caràcter personal en la Diputació Provincial de València, aprovat per Acord del Ple de la Corporació de 26 d'abril de 2022, aprovació definitiva en BOP núm. 127 de 5 de juliol de 2022, les Normes de Seguretat dels Usuaris dels Sistemes d'Informació, aprovades per Decret núm. 15873, de 27 de desembre de 2022, del president de la Diputació de València i per allò recollit en el glossari següent:

a) ***Accés remot**: Es considera accés remot el realitzat des de fora de les instal·lacions pròpies de l'organització, a través de xarxes de tercers.*

b) ***Administradors de seguretat delegats**: Els qui per delegació de l'Administrador de Seguretat dels Sistemes d'Informació TIC assumeixen, en l'àmbit de les seues competències funcionals, determinades atribucions d'aquest responsable* (article 30 del Reglament de política de seguretat i de la protecció de dades de caràcter personal).

c) ***Fortificació de seguretat**. La fortificació o configuració de seguretat comprén el conjunt de tècniques que busquen millorar el nivell de seguretat d'un sistema sense alterar la capacitat per a exercir la seua tasca.*

d) ***CMDB** (Sigles en anglés de base de dades de la gestió de configuració): La CMDB és un repositori d'informació on es relacionen tots els components d'un sistema d'informació, ja siguen maquinari, programari, documentació, etc.*

e) ***Computació en el núvol (cloud computing)****: La provisió de serveis en el núvol és un model per a permetre l'accés per xarxa, de manera pràctica i sota demanda, a un conjunt de recursos de computació configurables (per exemple, xarxes, servidors, emmagatzematge, aplicacions i serveis) que poden ser subministrats i desplegats ràpidament amb una mínima gestió o interacció amb el proveïdor de servei. [NIST SP-800-145]*

f) ***Contrasenya****: Informació confidencial, sovint composta d'una cadena de caràcters, que es pot usar en l'autenticació d'un usuari, entitat o recurs.*

g) ***Declaració d'aplicabilitat****: Document formal firmat pel responsable de Seguretat dels Sistemes d'Informació on consten les mesures de seguretat que han d'implementar-se en un sistema d'informació.*

h) ***Desastre:*** *S'entén per desastre qualsevol esdeveniment accidental, natural o malintencionat que interromp les operacions o els serveis habituals d'una organització durant el temps suficient com per a veure's afectada aquesta de manera significativa.*

i) ***Domini de seguretat****: Conjunto de sistemes d'informació sotmesos a una Política de Seguretat comuna, és a dir, homogenis des del punt de vista de les mesures de seguretat que cal aplicar.*

j) ***Firewall (tallafocs)****: Aquell sistema format per aplicacions, dispositius o combinació d'aquests, encarregat de fer complir una política de control d'accés en les comunicacions entre dispositius de xarxa segons una política de seguretat existent.*

k) ***Interconnexió de sistemes d'informació****: Es produeix una connexió quan es proveeixen els medis físics i lògics de transmissió adequats i susceptibles de ser emprats per a l'intercanvi d'informació. Es produeix*

una interconnexió de sistemes quan existeix una connexió i s'habiliten fluxos de comunicació entre aquests.

l) ***Responsables de seguretat delegats**: Els qui per delegació del responsable de Seguretat dels Sistemes d'Informació assumeixen, en l'àmbit de les seues competències funcionals, determinades atribucions d'aquest responsable (art*. 28 Reglament de política de seguretat i de la protecció de dades de caràcter personal).

m) ***Responsables del sistema delegats**: Els qui per delegació del responsable dels Sistemes d'Informació TIC assumeixen, en l'àmbit de les seues competències funcionals, determinades atribucions d'aquest responsable (art*. 29 Reglament de política de seguretat i de la protecció de dades de caràcter personal).

2. NORMATIVA INTERNA DE SEGURETAT PER AL PERSONAL TÈCNIC DELS SISTEMES D'INFORMACIÓ TIC

A l'efecte de la present normativa es considera **personal tècnic dels sistemes d'informació TIC** tota persona la comesa professional de la qual consistisca en l'anàlisi, el disseny o el desenvolupament de projectes tecnològics, la programació, manteniment, suport tècnic i gestió dels diferents components tecnològics dels sistemes d'informació TIC. S'hi inclou també el personal amb atribucions o responsabilitats professionals en matèria de seguretat dels sistemes d'informació TIC.

En la present normativa s'estableixen les directrius generals de seguretat que impliquen el personal tècnic, la qual cosa no esgota ni restringeix l'entorn de seguretat dels sistemes d'informació TIC, sinó que completa la resta de disposicions normatives internes de la Diputació de València que, elaborades també amb l'objectiu de la seguretat d'aquests sistemes, vagen dirigides a altres perfils de destinataris.

De conformitat amb el que es disposa en l'article 3 del Reglament de política de seguretat i de la protecció de dades de caràcter personal de la Diputació de València, les presents normes són aplicables a tots els sistemes d'informació TIC que siguen de titularitat de la Diputació de València o la gestió o la responsabilitat de la qual tinga encomanada.

N/SEG/TEC-001 ENTORN DE SEGURETAT DELS SISTEMES D'INFORMACIÓ TIC

L'entorn de seguretat dels sistemes d'informació TIC comprén el conjunt de mesures de caràcter tècnic i organitzatiu que resulten d'aplicació per a preservar la seguretat dels diferents elements o actius que integren aquests sistemes.

N/SEG/TEC-001-1 MESURES DE SEGURETAT

Les **condicions bàsiques de seguretat** que hauran d'estar presents en **tots els sistemes d'informació** seran:

- Els principis bàsics i requisits mínims de seguretat recollits en l'Esquema Nacional de Seguretat.

- Les mesures de seguretat dels articles i de l'Annex II de l'Esquema Nacional de Seguretat establides per als sistemes d'informació de categoria BÀSICA i que afecten a totes les dimensions de seguretat.

- En l'àmbit de la protecció de dades personals, s'atendrà al que es disposa en la disposició addicional primera de la Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals.

Una vegada establida la seguretat bàsica i després de l'avaluació del sistema, serà necessari implementar aquelles mesures de seguretat corresponents a la categoria del sistema.

La seguretat també podrà veure's incrementada, una vegada millorada, en aquells supòsits que així ho reclame la criticitat d'un sistema d'informació, o per decidir-ho així l'organització a través del Comité de Seguretat TIC mitjançant l'establiment de línies estratègiques de seguretat dels sistemes d'informació.

Correspon al **responsable de Seguretat dels Sistemes d'Informació** determinar les mesures de seguretat concretes per a cada sistema d'informació, d'acord amb la normativa d'aplicació, com també la supervisió sistemàtica i

periòdica de les mesures implementades. Les condicions concretes de seguretat es plasmaran en la **Declaració d'Aplicabilitat** corresponent**.**

Les condicions de seguretat establides en la Declaració d'Aplicabilitat s'implementaran en cada sistema d'informació afectat. Serà obligació de cada **responsable del sistema delegat** assegurar que els requisits de seguretat s'integren adequadament en el seu àmbit, i dels **administradors de seguretat delegats** la responsabilitat de dur a terme la seua implantació, gestió i manteniment.

Quan alguna mesura de seguretat o salvaguarda comporte especial dificultat en la seua implementació, segons el parer dels administradors de seguretat delegats afectats, aquests hauran de realitzar un estudi de l'abast i la viabilitat tècnica i econòmica de la implementació. Amb aquest informe el Comité de Seguretat TIC haurà de decidir la fórmula d'execució més viable i el termini per a dur-la a terme, i considerarà els recursos necessaris.

Una vegada que aquesta mesura o salvaguarda es trobe implantada i plenament operativa, l'administrador de seguretat delegat afectat emetrà una declaració en la qual conste la seua entrada en funcionament.

Haurà d'elaborar-se un procediment en el qual s'establisquen les pautes d'actuació per a garantir que al responsable de Seguretat dels Sistemes d'Informació li arriba la informació necessària per a poder determinar les mesures de seguretat concretes que són aplicables a cada sistema d'informació, com també que cap sistema d'informació no entre en operació sense adoptar les mesures de seguretat que li siguen aplicables.

N/SEG/TEC-001-2 ACTIUS DELS SISTEMES D'INFORMACIÓ

Es mantindrà un inventari actualitzat de tots els elements del sistema, i s'hi detallarà la seua naturalesa i se n'identificarà el responsable; és a dir, la persona que és responsable de les decisions relatives a aquest.

A l'efecte de valoració de riscos, es determinaran en cada sistema els actius més valuosos i les seues amenaces més probables.

Cada responsable, respecte dels seus actius, haurà de:

- Incorporar cada element nou a l'inventari, i proporcionar la informació pertinent i l'establiment les dependències entre actius.
- Mantindre la informació de l'actiu actualitzada.
- Dur a terme la valoració de riscos.

N/SEG/TEC-001-3 SEGURETAT EN SERVEIS DE TERCERS

L'entorn de seguretat dels sistemes d'informació que resulte d'aplicació ho serà amb independència que es recórrega a la contractació de serveis externs. La responsabilitat del compliment de les condicions de seguretat de tot o part d'un sistema d'informació de la Diputació de València correspon exclusivament a aquesta i no pot ser transferida a tercers, per la qual cosa es disposaran les mesures necessàries per a poder exercir la seua responsabilitat i mantindre el control en tot moment. Per això, el personal tècnic que participe en la contractació d'aquesta mena de serveis atendrà el que es preveu en l'apartat N/SEG/TEC-021-2.

Quan es tracte de supòsits de *cloud computing* caldrà ajustar-se, a més, al que es preveu en l'apartat N/SEG/TEC-010.

En cas que s'utilitzen plataformes, programes o serveis **sota el control i la gestió d'un altre organisme públic** —diferent domini de seguretat— com a part dels recursos (actius) per a prestar un servei i/o explotar una informació, s'haurà de formalitzar amb aquest organisme un conveni o acord on conste el marc general de seguretat a aplicar i la responsabilitat de cada entitat pública.

N/SEG/TEC-001-4 SEGURETAT EN INTERCONNEXIÓ DE SISTEMES D'INFORMACIÓ

Quan s'interconnecten sistemes en els quals la identificació, autenticació i autorització tinguen lloc en diferents dominis de seguretat, sota diferents responsabilitats, en els casos en què siga necessari, les mesures de seguretat locals s'acompanyaran dels acords de col·laboració corresponents que delimiten mecanismes i procediments per a l'atribució i l'exercici efectius de les responsabilitats de cada sistema.

Prèviament a la interconnexió dels sistemes:

- Es documentarà la necessitat d'interconnexió i es farà constar: les característiques de la interfície, els requisits de seguretat i protecció de dades, la naturalesa de la informació intercanviada i el tipus d'informació que es requereix intercanviar entre els dos sistemes.
- La interconnexió haurà d'autoritzar-la el responsable dels Sistemes d'Informació.
- La interconnexió estarà subjecta a l'anàlisi i gestió de riscos de la seguretat. Un augment en el nivell de risc a causa de la interconnexió requerirà un informe del responsable de Seguretat dels Sistemes d'Informació.

La interconnexió de dos sistemes es realitzarà mitjançant un Sistema de Protecció de Perímetre (SPP). Aquest SPP serà una combinació de recursos de maquinari i/o programari que es denominarà Dispositiu de Protecció de Perímetre (DPP), la finalitat del qual és mediar en el trànsit d'entrada i eixida en els punts d'interconnexió dels sistemes.

Haurà d'elaborar-se un procediment per a la interconnexió dels sistemes, on s'establisquen les especificacions tècniques de l'entorn de seguretat de sistemes interconnectats.

N/SEG/TEC-001-5 SEGURETAT DE COMUNICACIONS, NOTIFICACIONS I PUBLICACIONS ELECTRÒNIQUES

Les comunicacions electròniques a les quals es refereix la Llei 39/2015 (PAC) adoptaran les condicions de seguretat previstes en la present normativa que resulten apropiades per a garantir:

- La constància de la transmissió i recepció de la comunicació electrònica, de les dates en les quals es van realitzar, com també del contingut íntegre d'aquestes.
- La identificació fidedigna del remitent i destinatari de la comunicació.

D'igual forma, les notificacions i publicacions electròniques de resolucions i actes administratius adoptaran les condicions de seguretat previstes en la present normativa que resulten apropiades per a:

- Assegurar l'autenticitat de l'organisme que el publique.
- Assegurar la integritat de la informació publicada.

- Deixar constància de la data i l'hora de la posada a la disposició de l'interessat de la resolució o acte objecte de publicació o notificació, així com de l'accés al seu contingut.
- Assegurar l'autenticitat del destinatari de la publicació o notificació.

N/SEG/TEC-002 PLANTEJAMENT INTEGRAL DE LA SEGURETAT

Es disposarà d'un conjunt de documents aprovats pel Comité de Seguretat TIC referits al plantejament integral de la seguretat del sistema. La documentació elaborada a aquest efecte serà, com a mínim, la següent:

a) Documentació de les instal·lacions. Es detallaran les instal·lacions, i es requerirà:

- La classificació de la instal·lació, atenent el que es disposa en l'apartat N/SEG/TEC-017
- Les àrees existents
- Els punts d'accés

b) Documentació del sistema. Es disposarà d'un inventari actualitzat del sistema d'informació. L'inventari contindrà una descripció:

- Dels equips
- De les xarxes internes existents, i els elements de connexió a l'exterior
- Dels punts d'accés al sistema
- Dels responsables dels elements; entenent com a responsable la persona que és responsable de les decisions relatives a cada element

c) Documentació de línies de defensa. Es disposarà d'un inventari amb un esquema dels sistemes de seguretat del sistema d'informació. L'inventari contindrà una descripció:

- Dels elements d'interconnexió a altres xarxes
- Dels elements de defensa en les connexions a altres xarxes
- De les possibles tecnologies diferents per a previndre vulnerabilitats que pogueren perforar simultàniament diverses línies de defensa

d) Documentació del sistema d'identificació i autenticació d'usuaris. Es detallaran els sistemes d'identificació i autenticació d'usuaris per a cada sistema o servei. Es precisaran:

- El mecanisme d'autenticació a cada sistema o servei
- On s'emmagatzemen les contrasenyes

e) Documentació dels controls tècnics interns. Es detallarà com es controlen les dades una vegada en els sistemes. Es descriurà la validació de dades d'entrada, eixida i dades intermèdies.

f) Documentació del sistema de gestió amb actualització i aprovació periòdica. Es detallarà com es gestionen els elements abans enumerats, amb quina freqüència es revisen, qui és l'encarregat de la tasca i qui és el responsable de la seua aprovació.

N/SEG/TEC-003 AUTORITZACIONS

Sense perjudici d'altres referències d'autorització recollides en aquesta o una altra normativa interna, s'expressen a continuació per a cadascun dels següents tipus de component o actuació del sistema d'informació, la persona o punt de contacte per a la seua autorització:

a) Correspon al **responsable dels Sistemes d'Informació** o **responsable del Sistema delegat** l'autorització per a:

- La utilització d'instal·lacions, tant habituals com alternatives.
- L'entrada d'equips en producció, en particular, equips que involucren criptografia.
- La instal·lació en el sistema de qualsevol element físic o lògic.
- L'entrada d'aplicacions en producció.
- La recuperació d'informació de les còpies de seguretat, en els casos en què no siga a sol·licitud dels usuaris de la informació.

b) Correspon al **responsable dels Sistemes d'Informació** o **responsable del Sistema delegat**, prèvia autorització del **responsable de la Informació o del servei corresponent,** l'autorització per a:

- L'accés d'una entitat (usuari o procés) al sistema d'informació.
- La utilització d'equips portàtils i mòbils.
- La utilització de mitjans de comunicació, habituals i alternatius.
- La recuperació d'informació de les còpies de seguretat, quan siga a sol·licitud dels usuaris de la informació.

Tot procés d'autorització estarà degudament documentat, haurà d'haver-hi un model de sol·licitud (formulari) que continga la informació necessària perquè el responsable puga prendre la decisió sobre l'autorització de manera adequada.

N/SEG/TEC-004 ACCÉS LÒGIC

N/SEG/TEC-004-1 CONTROL D'ACCÉS

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

L'accés lògic i operatiu als sistemes d'informació de la Diputació de València es controlarà a través del programari de seguretat d'accés a la xarxa, com també a través dels mòduls de seguretat de les aplicacions específiques.

Els accessos al sistema respectaran, en qualsevol cas, els principis següents:

a) **Mínim privilegi**. Els privilegis de cada usuari es reduiran al mínim estrictament necessari per a complir les seues obligacions.
b) **Necessitat de conéixer**. Els privilegis es limitaran de manera que els usuaris només accediran al coneixement d'aquella informació requerida per a complir les seues obligacions.
c) **Capacitat d'autoritzar**. Només i exclusivament el personal amb competència per a això podrà concedir, alterar o anul·lar l'autorització d'accés als recursos, conforme als criteris establits pel seu responsable.

Es disposarà de mecanismes per al control de tots els accessos (usuaris o processos) al sistema d'informació, siguen locals o remots. Aquests mecanismes hauran de garantir:

• Que tot accés estiga prohibit, excepte concessió expressa, de manera que s'impedisca la seua utilització, tret de les entitats que gaudisquen de drets d'accés suficients. Particularment, es controlarà l'accés als components del sistema i als seus fitxers o registres de configuració.

• Que un usuari no puga accedir a recursos amb drets diferents dels autoritzats.

• Que cada entitat (usuari o procés) que accedeix al sistema té un identificador singular, que permet saber qui ha fet alguna cosa i quina cosa ha fet.

• Que es definisquen per a cada entitat a la qual es necessita accedir, amb quins drets i sota quina autorització.

• L'existència d'una relació del personal autoritzat per a concedir, alterar o anul·lar l'accés autoritzat sobre els recursos, conforme als criteris establits per la normativa interna.

• L'existència d'un registre de les entitats responsables de cada identificador que permeta saber a qui correspon cada identificador i els permisos o drets que té, com també qui ha sigut el seu autoritzador.

• La inhabilitació de l'identificador quan l'usuari deixa l'organització cessa en la funció per a la qual es requeria el compte d'usuari o quan la persona que la va autoritzar dona ordre en sentit contrari.

• Que, no obstant la inhabilitació anterior, l'identificador es manté durant el període necessari per a atendre les necessitats de traçabilitat dels registres d'activitat associats a aquests (període de retenció).

• La segregació de funcions i tasques crítiques en els sistemes crítics i en els de categoria MITJANA o superior, de manera que s'exigisca la concurrència de dues persones o més per a fer tasques crítiques, i anul·lar la possibilitat que un sol individu autoritzat puga abusar dels seus drets per a cometre alguna acció il·lícita. Com a mínim seran incompatibles: Desenvolupament amb operació del sistema, configuració i manteniment del sistema amb operació del sistema, auditoria o supervisió del sistema amb qualsevol altra funció.

Cap usuari final no haurà de tindre privilegis especials que li permeten configurar paràmetres de seguretat o administrar claus.

L'accés a les aplicacions i bases de dades ha de ser independent de l'accés al sistema operatiu.

Per a minimitzar el nombre d'accessos no autoritzats als sistemes es tindran en compte els aspectes següents:

• Fins que no s'haja completat amb èxit el procés d'autenticació, no s'haurà de mostrar cap mena d'informació relativa al sistema que puga ajudar a identificar-lo, com tampoc qualsevol altre tipus d'informació que en puga facilitar l'accés no autoritzat.

• Una vegada s'haja accedit correctament al sistema, s'haurà de mostrar un missatge que advertisca que l'ús del sistema només està permés a usuaris autoritzats.

• La validació de la informació d'entrada es realitzarà únicament quan s'hagen completat totes les dades d'entrada. Si ocorre alguna condició d'error, el sistema no haurà d'indicar en cap cas la part de la dada que és incorrecta.

• Sempre que siga possible, s'hauran d'utilitzar protocols de comunicació que permeten l'enviament de les credencials d'usuari de forma xifrada per a evitar que siguen capturades en algun punt intermedi de la comunicació.

N/SEG/TEC-004-2 ACCÉS REMOT

En els accessos remots s'observaran les mateixes condicions que les assenyalades per a l'accés local i es protegirà el canal d'accés remot amb les mesures indicades en l'apartat N/SEG/TEC-006 per a la protecció de les comunicacions.

El Comité de Seguretat TIC decidirà quines activitats poden realitzar-se remotament, com també aquelles que requerisquen autorització prèvia, qui pot autoritzar-les i, si s'escau, el període d'autorització. De tot això es deixarà constància en els procediments pertinents.

A fi de limitar el que es pot fer en remot caldrà establir un filtre, bé en el servidor, bé en l'equip client.

N/SEG/TEC-004-2-1 TELETREBALL

Les directrius recollides en el present apartat són complementàries de les disposicions contingudes en l'apartat N/SEG/TEC-002-11 MODALITAT DE TELETREBALL de les Normes de Seguretat per als usuaris dels Sistemes d'Informació, aprovades per Decret núm. 15873 de 27 de desembre de 2022, del president de la Diputació de València.

La persona que s'aculla a la modalitat de teletreball haurà de disposar d'un sistema de comunicació i connectivitat que complisca amb les característiques tècniques que determine el Servei d'Informàtica.

El Servei d'Informàtica entregarà les credencials d'accés perquè els usuaris puguen accedir a través de les diferents opcions que s'ofereixen en la modalitat de teletreball.

El Servei d'Informàtica subministrarà l'equipament i les aplicacions informàtiques que resulten adequades per a la prestació del servei sota la modalitat de teletreball.

Aquest equipament d'aplicacions informàtiques les realitzarà a través de tres mètodes:

- Webs corporatives: Web d'accessos a través d'internet, on no es requerirà cap característica especial en els equips, només s'utilitzarà l'usuari-contrasenya i el Múltiple Factor d'Autenticació (MFA) que l'organització utilitze.

- Citrix: Entorn on s'utilitzarà un llistat d'aplicacions publicades, diferents per a cada usuari en funció dels seus rols o autoritzacions donades pels responsables de l'organització.

En aquesta opció caldrà disposar d'aplicacions informàtiques instal·lades en l'equip per a poder connectar a l'entorn de Citrix mitjançant usuari-contrasenya i MFA.

- VPN: Entorn on es realitzarà la connexió mitjançant protocol VPN cap a l'organisme. Aquest entorn haurà de ser autoritzat pel personal responsable dels diferents departaments.

L'equipament informàtic i les aplicacions informàtiques subministrades seran d'ús exclusivament laboral. Així mateix, la Diputació de València subministrarà un número de telèfon IP o mòbil corporatiu, d'acord amb la peculiaritat de les funcions i tasques del lloc.

La persona que preste el seu servei mitjançant teletreball serà la responsable de custodiar i retornar l'equipament en les mateixes condicions que li van ser subministrat.

Correspondrà a la persona teletreballadora la comunicació de les incidències que puguen produir-se en l'equip informàtic.

En el supòsit que es produïsquen deficiències o desperfectes derivats d'un ús inadequat o negligent, la Diputació podrà exigir les responsabilitats oportunes.

Així mateix, quan es produïsca un mal funcionament en l'equip informàtic o en les aplicacions hi instal·lades, així com en el servidor o les plataformes que permeten el teletreball, que impedisquen el treball des de l'oficina a distància i

que no puga ser solucionat el mateix dia en què van ocórrer o l'endemà, la persona teletreballadora haurà de reincorporar-se al seu centre de treball, i reprendrà l'exercici de la seua activitat en la modalitat de teletreball quan quede resolt el problema tècnic.

La Diputació de València haurà de dotar les persones que desenvolupen la seua activitat sota la modalitat de teletreball d'un servei informàtic de suport tècnic per a la resolució d'incidències puntuals.

El personal en aquesta modalitat haurà de custodiar els actius que l'organització li preste per al desenvolupament del seu treball, per la qual cosa haurà de seguir les indicacions de seguretat recollides en la normativa interna en la matèria.

El trànsit s'haurà de xifrar mitjançant configuracions i criptologia que haja sigut definida per qualsevol guia o manual de fortificació, ja siga del fabricant, del CCN, del CIS o del NIST.

Si la utilització no es produeix de manera constant, l'accés remot haurà de trobar-se inhabilitat i habilitar-se únicament quan siga necessari.

S'hauran de recollir registres d'auditoria d'aquesta mena de connexions.

S'hauran d'utilitzar guies o manuals de configuració per a establir una fortificació dels actius, referint per actiu qualsevol actiu que forme part del procés d'accés remot, tant d'actius perimetrals, interns, conscienciació del personal, com de dispositius mòbils, com també seguir l'estratègia de seguretat d'accés remot que s'haja establit en l'organisme.

N/SEG/TEC-004-3 IDENTIFICACIÓ D'USUARIS

La identificació dels usuaris del sistema s'efectuarà d'acord amb el que s'indica tot seguit:

Cada entitat (usuari o procés) que accedeix al sistema comptarà amb un identificador singular que en permeta conéixer el destinatari i els drets d'accés que rep, i també les accions realitzades per cada entitat.

Els comptes d'usuari es gestionaran de la forma següent:

- Cada compte estarà associat a un identificador únic.
- Els comptes han de ser inhabilitats en els casos següents: Quan l'usuari deixa l'organització; quan l'usuari cessa en la funció per a la qual es requeria el compte d'usuari, o, quan la persona que el va autoritzar dona ordre en sentit contrari. S'automatitzaran el màxim possible les tasques que permeten la inhabilitació immediata dels comptes quan es produïsquen les circumstàncies d'inhabilitació.

Els comptes es retindran durant el període necessari per a atendre les necessitats de traçabilitat dels registres d'activitat associats a ells. Aquest període es denominarà període de retenció. Els períodes de retenció seran determinats pel Comité de Seguretat TIC.

La identificació de l'usuari permetrà al responsable del sistema, al responsable de la seguretat o als seus administradors delegats respectius, singularitzar la persona associada a aquest, així com les seues responsabilitats en el sistema.

Les dades d'identificació seran utilitzades pel sistema per a determinar els privilegis de l'usuari conforme als requisits de control d'accés establits en la documentació de seguretat.

S'assegurarà l'existència d'una llista actualitzada d'usuaris autoritzats i mantinguda per l'administrador del sistema/de la seguretat del sistema.

N/SEG/TEC-004-4 MECANISMES D'AUTENTICACIÓ

Les instàncies del factor o els factors d'autenticació que s'utilitzen en el sistema es denominaran **credencials**. En els sistemes d'informació TIC de la Diputació de València podran utilitzar-se els factors d'autenticació següents:

a) Una cosa que se sap. Contrasenyes o claus concertades.

b) Una cosa que es té. Components lògics o dispositius físics.

c) Una cosa que s'és. Elements biomètrics.

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

En aquells sistemes no crítics i de categoria BÀSICA, com a principi general, s'admetrà l'ús de qualsevol mecanisme d'autenticació sustentat en un sol factor. S'exigirà l'ús d'almenys de dos factors d'autenticació quan es tracte de sistemes crítics o de categoria MITJANA i superior.

En sistemes de categoria MITJANA no està aconsellat l'ús de claus concertades, en el cas que s'utilitzen, es permetran aquelles que estiguen formades almenys de 8 caràcters alfanumèrics. Si aquests últims són generats de manera aleatòria

o pseudoaleatòria, hauran de posseir la suficient seguretat com per a evitar repeticions o hipòtesis sobre el seu possible valor. L'ús de claus concertades no es permetrà en sistemes crítics o de categoria ALTA.

Quan es tracte de sistemes crítics o de categoria ALTA, els mecanismes d'autenticació es basaran en dispositius físics personalitzats o mitjançant dispositius que facen ús de patrons biomètrics. En el cas d'utilitzar un patró biomètric es requerirà la utilització d'un segon factor d'autenticació *token* o clau segura (generada de manera aleatòria i amb una longitud almenys de 8 caràcters alfanumèrics). En el cas de l'ús d'utilització d'«una cosa que es té», es requerirà l'ús d'elements criptogràfics *hardware,* usant algoritmes i paràmetres acreditats pel CCN.

Per a donar seguretat a les credencials s'atendrà, com a mínim, el següent:

Les credencials s'activaran una vegada estiguen sota el control efectiu de l'usuari.

Les credencials estaran sota el control exclusiu de l'usuari.

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

Les credencials es canviaran amb la periodicitat marcada pel Comité de Seguretat TIC, atesa la categoria del sistema i el resultat de l'anàlisi de riscos. D'igual manera, les credencials se suspendran després d'un període de no utilització definit pel Comité.

Les credencials seran inhabilitades —i podran ser regenerades, si escau— quan conste o se sospite la seua pèrdua, compromís o revelació a entitats (persones, equips o processos) no autoritzades.

Les credencials es retiraran i seran deshabilitades quan l'entitat (persona, equip o procés) que les autentica acabe la seua relació amb el sistema o quan la persona que les va autoritzar done l'ordre en sentit contrari.

Abans d'autoritzar l'accés, la informació presentada pel sistema serà la mínima imprescindible perquè l'usuari s'autentique, i evitar tot allò que puga, directament o indirectament, revelar informació sobre el sistema o el compte, les seues característiques, la seua operació o el seu estat. Les credencials solament es validaran quan es tinguen totes les dades necessàries i, si es rebutgen, no s'informarà del motiu del rebuig.

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

- Mitjançant la presentació física de l'usuari i verificació de la seua identitat concorde a la legalitat vigent, davant un funcionari habilitat per a això.
- De forma telemàtica, mitjançant DNI electrònic o un certificat electrònic qualificat.
- De manera telemàtica, utilitzant altres sistemes admesos legalment per a la identificació dels ciutadans dels contemplats en la Llei 39/2015 (LPAC).

El nombre d'intents permesos serà limitat, es bloquejarà l'oportunitat d'accés una vegada superat aquest nombre i es requerirà una intervenció específica per a reactivar el compte, la qual es descriurà en la documentació.

Quan l'usuari tinga diferents rols davant el sistema (com a ciutadà o usuari final, com a treballador de l'organisme o com a administrador dels sistemes, per exemple) rebrà identificadors singulars per a cada perfil, de manera que es recapten sempre els registres d'activitat corresponents, i es delimiten els privilegis corresponents a cada perfil.

El sistema informarà l'usuari dels seus drets o obligacions immediatament després d'obtindre l'accés.

Es requerirà una contrasenya d'un sol ús (OTP, en anglés) com a complement a la contrasenya d'usuari o s'utilitzaran certificats qualificats com a mecanisme d'autenticació, i aquest estarà protegit per un segon factor del tipus PIN o biomètric.

Es registraran els accessos amb èxit i els fallits.

S'informarà l'usuari de l'últim accés efectuat amb la seua identitat.

N/SEG/TEC-004-5 ÚS DE CONTRASENYES

Sense perjudici del que s'estableix en l'apartat anterior "mecanismes d'autenticació", quan el mecanisme d'autenticació usat per a l'accés a determinats sistemes o serveis consistisca en contrasenyes, es compliran les condicions següents:

Les contrasenyes, mentre estiguen vigents, s'emmagatzemaran amb algun mètode de protecció que en garantisca la confidencialitat i integritat, és a dir, de manera inintel·ligible, que no es puga entendre.

La clau o identificació d'accés, atorgada pel Servei d'Informàtica en el moment de l'alta de l'usuari, li serà comunicada de manera segura. No s'han d'incloure en correus electrònics o en altres mitjans de comunicació electrònica no segurs, ni comunicades per telèfon. És responsabilitat de l'usuari efectuar els canvis d'aquesta, d'acord amb la periodicitat i sintaxi establida. Es podrà establir un sistema de generació automàtica de claus d'accés amb les garanties de seguretat degudes.

La contrasenya facilitada a l'usuari pel Servei d'Informàtica serà provisional i haurà de forçar el seu canvi immediat, després del primer inici de sessió, per una altra personalitzada per l'usuari.

L'usuari podrà efectuar el canvi voluntari de la clau sempre que ho desitge. D'igual manera, l'administrador del sistema, aplicació o producte utilitzat per l'usuari, podrà efectuar el canvi de clau si es produeix alguna incidència que aconselle aquest canvi.

En el moment del canvi no estarà permesa la reutilització del valor emprat per a les últimes claus, segons l'antiguitat que s'hi especifique.

• La clau de l'usuari no s'haurà de mostrar en pantalla mentre s'introdueix.

• Les contrasenyes, perquè siguen vàlides, hauran de tindre una longitud mínima de sis posicions i consistir en una combinació de caràcters alfanumèrics.

• S'ha d'evitar la característica "Recordar Contrasenya" existent en algunes aplicacions i formularis.

• Les contrasenyes hauran de forçar el seu canvi periòdicament. Han d'existir mecanismes d'expiració i caducitat de contrasenyes per a obligar els usuaris al canvi d'aquesta.

• S'establirà un nombre d'intents d'accés fallits. Una vegada superat aquest es produirà el bloqueig automàtic de l'usuari.

• Les decisions sobre límit d'intents d'accés fallits, la periodicitat per al canvi de contrasenyes i la política de qualitat de les contrasenyes seran adoptades pel Comité de Seguretat TIC, atesa la categoria del sistema i el resultat de l'anàlisi de riscos. El producte d'aquestes decisions es documentarà a través del procediment per a l'assignació, distribució i emmagatzematge, si s'escau, dels mecanismes utilitzats per a la identificació i autenticació en els sistemes d'informació.

• Totes les contrasenyes per defecte dels sistemes o aplicacions han de ser canviades quan no siguen necessàries.

• S'imposaran normes de complexitat mínima i robustesa contra atacs d'endevinació, segons guies CCN-STIC.

• El Comité de Seguretat TIC decidirà sobre l'oportunitat que alguns usuaris puguen utilitzar programes gestors de contrasenyes.

N/SEG/TEC-005 MONITORATGE

El monitoratge és l'activitat consistent en la recopilació d'informació, a través de *programari* o d'un altre tipus de mecanismes sensors, de l'entorn d'un sistema d'informació per a la seua anàlisi, control o simple obtenció d'evidències posterior.

Tots els equips que compten amb un rellotge intern estaran sincronitzats entre si per a garantir la precisió dels successos registrats i permetre la correlació dels diferents esdeveniments.

Aquells successos registrats que puguen ser susceptibles de constituir evidències en processos judicials o en procediments administratius sancionadors, hauran de comptar amb totes aquelles garanties tecnològiques que proporcionen el caràcter de prova vàlida a aquests successos.

N/SEG/TEC-005-1 REGISTRES D'ACTIVITAT

Hauran d'existir, com a mínim, els tipus de registres d'activitat següents:

a) **Registre d'activitat d'usuaris en el sistema**. Es registraran les activitats dels usuaris en el sistema, de manera que el registre indicarà qui efectua l'activitat, quan l'efectua i sobre quina informació. S'inclourà l'activitat dels usuaris i, especialment, la dels operadors i administradors quan puguen accedir a la configuració i actuar en el manteniment del sistema. Hauran de registrar-se les activitats realitzades amb èxit i els intents fracassats.

La determinació de quines activitats han de registrar-se i amb quins nivells de detall s'adoptarà a la vista de l'anàlisi de riscos realitzada sobre el sistema.

El registre d'activitat anirà associat al compte d'usuari en els casos a què es refereix l'apartat N/SEG/TEC-004-1.

b) **Registre d'accessos a tractaments de dades personals pertanyents a categories especials o amb risc alt**. En tots aquells tractaments de dades personals pertanyents a les categories especials o aquells que llancen un resultat d'un risc alt segons l'anàlisi de riscos, haurà d'habilitar-se un registre automàtic de tots els accessos, encara que l'intent d'accés no haja tingut èxit. Aquest registre contindrà, com a mínim, la informació següent: La identificació de l'usuari, la data i l'hora en què es va realitzar, el fitxer al qual es va accedir, el tipus d'accés i si ha sigut autoritzat o denegat. En el cas que l'accés haja sigut autoritzat, caldrà guardar la informació que permeta identificar el registre accedit. El responsable de Seguretat s'encarregarà de revisar almenys una vegada al mes la informació de control registrada i elaborarà un informe de les revisions realitzades i els problemes detectats. El període mínim de conservació de les dades registrades serà de **dos anys**.

c) **Registre d'evidències d'activitat en un procediment sancionador administratiu o en un procés judicial**. Es registraran les activitats dels usuaris, i es retindrà la informació necessària per a monitorar, analitzar, investigar i documentar activitats indegudes o no autoritzades, tant a nivell operatiu com d'administració, cosa que permetrà identificar a cada moment la persona que actua. Es registrarà aquella evidència que puga, posteriorment, sustentar una demanda judicial, o fer-li front, quan un

incident puga portar a actuacions disciplinàries sobre el personal intern, sobre proveïdors externs o a la persecució de delictes.

El Comité de Seguretat TIC podrà acordar la creació d'uns altres registres d'activitat si així ho estima convenient.

El delegat de Protecció de Dades i el Departament de Protecció de Dades i Seguretat de la Informació, en l'exercici de les seues competències, sempre tindran accés als registres descrits en els apartats anteriors i a qualssevol altres que s'hi puguen a criteri del Comité de Seguretat TIC.

El sistema es configurarà de manera que el contingut d'aquests registres no puga modificar-se, com tampoc la garantia de protecció davant l'eliminació per persones no autoritzades. En qualsevol cas, i com que també es recull l'activitat dels operadors i administradors del sistema, es garantirà que els operadors i administradors mateixos no puguen modificar-los o eliminar-los.

Quan es tracte dels registres descrits en els apartats b) i c), es configuraran de manera que la seua eliminació requerisca el concurs de dues persones: el responsable de Seguretat dels Sistemes d'Informació i el responsable dels Sistemes d'Informació. Haurà de deixar-se constància documental de cada eliminació del contingut d'aquests registres.

Els mecanismes que permeten els registres dels apartats b) i c) estaran sota el control directe del responsable de Seguretat dels Sistemes d'Informació sense que s'haja de permetre la desactivació ni la manipulació d'aquests. D'igual manera, l'accés als registres citats i la seua custòdia correspondran al responsable de Seguretat dels Sistemes d'Informació, a excepció del que es disposa en aquest mateix apartat respecte de les competències del delegat de Protecció de Dades i el Departament de Protecció de Dades i Seguretat de la Informació.

S'elaborarà un inventari dels registres d'activitat, on, a més, s'indicarà el personal autoritzat al seu accés o eliminació. I el període de retenció d'aquests.

Es disposarà d'un pla per a garantir la capacitat d'emmagatzematge de registres atenent el seu volum i la política de retenció, com també d'un procediment per a l'eliminació dels registres després del període estipulat de retenció, incloses les còpies de seguretat. Les còpies de seguretat s'ajustaran als mateixos requisits establits per als registres en viu.

N/SEG/TEC-005-2 MONITORATGE OPERATIU DE LA SEGURETAT

S'hauran d'establir les rutines d'operació de la seguretat que permeten la prevenció, detecció i correcció precoç de possibles incidents de seguretat, així com monitorar, detectar i informar automàticament quan una norma o política de seguretat haja sigut violada, com ara els canvis en la configuració de seguretat aprovada prèviament. L'aplicació d'aquesta norma haurà de desencadenar, sempre que siga possible, accions automàtiques.

A l'efecte de seguretat, s'haurà de fer ús del monitoratge del trànsit de xarxa amb dos grans objectius: primer, per a detectar situacions anòmales que puguen introduir riscos en la seguretat corporativa i, segon, dins de la gestió d'un incident, per a identificar les activitats a través de la xarxa d'un intrús o un programari nociu concret.

S'utilitzarà el monitoratge del trànsit de xarxa amb els objectius específics següents:

• Estudiar la informació transmesa a través d'un protocol per a identificar la criticitat de la informació enviada per la xarxa i aplicar així salvaguardes, en cas de ser requerides.

• Comprovar el tipus d'informació que pot ser observada per un altre usuari amb possibilitat de connectar-se a la mateixa xarxa per a identificar els riscos de robatori de dades als quals ens exposem.

• Definir perfils de trànsit que ens permeten identificar anomalies en la xarxa.

• Identificar el trànsit no conegut pels administradors de la xarxa i determinar si és legítim o no.

• Investigar un possible incident o investigar el trànsit relacionat amb un incident de seguretat confirmat per a procedir a realitzar la resposta adequada (contenció, erradicació…).

• Capturar informació sensible.

Se seguiran les especificacions contingudes en la Guia CCN-STIC-435 pel que fa al procés d'anàlisi de trànsit de xarxa, selecció i implantació d'eines i contramesures.

També s'utilitzarà el monitoratge del trànsit d'hosts amb l'objectiu de previndre atacs d'escalat de privilegis.

El sistema disposarà d'eines de detecció o prevenció d'intrusions basades en regles.

Es disposarà d'un sistema automàtic de recol·lecció d'esdeveniments de seguretat que permeta la correlació d'aquests.

Es disposarà de solucions de vigilància que permeten determinar la superfície d'exposició en relació amb vulnerabilitats i deficiències de configuració.

L'accés a les eines de captura i els registres generats per aquestes, especialment als fitxers de captura de trànsit, ha de romandre estrictament restringit al personal que exercisca les tasques de monitoratge. Addicionalment, la protecció d'aquests registres és vital per a l'organització, a causa de la naturalesa de la informació que poden emmagatzemar, per la qual cosa han de desplegar-se les mesures de seguretat necessàries en cada cas i eliminar els registres, una vegada hagen sigut processats.

N/SEG/TEC-005-3 MÈTRIQUES I INDICADORS

Hauran d'establir-se mecanismes que permeten conéixer a cada moment l'estat de la seguretat, millorar-lo i gestionar les despeses i inversions necessàries.

Les mètriques i els indicadors, que seran acordats pel Comité de Seguretat TIC, abastaran els tipus següents:

- **De compliment**. Per a conéixer el grau de cobertura d'una certa referència (pot ser una política interna, un reglament, un perfil, etc.).
- **D'eficàcia**. Per a conéixer l'acompliment d'una certa funció, des del punt de vista d'en quina mesura aconseguim els resultats abellits.
- **D'eficiència**. Per a conéixer l'acompliment d'una certa funció, des del punt de vista de si el consum de recursos, en termes d'hores i pressupostos, està proporcionat als resultats obtinguts.
- **D'impacte**. Per a traduir els incidents tècnics en conseqüències per a la missió última del sistema: Protecció d'una certa informació i prestació d'uns serveis determinats.

- **Predictius**. Els indicadors que anticipen el que passarà.
- **Explicatius**. Els que mesuren el passat. Són útils per a entendre el que ha ocorregut i poder reaccionar amb coneixement de causa.

Atesa la categoria de seguretat del sistema, es recopilaran les dades necessàries per a conéixer el grau d'implantació de les mesures de seguretat que resulten aplicables i, si escau, per a proveir l'informe anual requerit per l'article 32 de l'ENS.

Es recopilaran les dades precises que possibiliten avaluar el comportament del sistema de gestió d'incidents, d'acord amb la Instrucció Tècnica de Seguretat de Notificació d'Incidents de Seguretat i amb la guia CCN-STIC corresponent.

N/SEG/TEC-006 PROTECCIÓ DE LES COMUNICACIONS

N/SEG/TEC-006-1 SEGURETAT PERIMETRAL I FLUXOS D'I NFORMACIÓ

Es disposarà d'un sistema de tallafocs que separe la xarxa interna de l'exterior, de manera que tot el trànsit amb l'exterior passe a través del tallafocs. Només es permetrà el trànsit que haja sigut prèviament autoritzat. El perímetre concret, delimitat i acotat estarà reflectit en l'arquitectura del sistema.

La Instrucció Tècnica de Seguretat d'Interconnexió de Sistemes d'Informació determinarà els requisits establits en el perímetre que han de complir tots els components del sistema en funció de la categoria.

S'empraran algorismes i paràmetres autoritzats pel CCN per a les connexions.

S'empraran, en el perímetre, tecnologies diferents per a previndre vulnerabilitats que pogueren perforar simultàniament diverses línies de defensa.

Per als fluxos d'informació, el trànsit per la xarxa se segregarà perquè cada equip només tinga accés a la informació que necessita.

Si s'empren comunicacions sense fils, serà en un segment separat.

Els segments de xarxa s'implementaran per mitjà de xarxes d'àrea local virtuals (Virtual Local Area Network, VLAN).

La xarxa que conforma el sistema haurà de segregar-se en diferents subxarxes, i contemplarà com a mínim:

• Usuaris.
• Serveis.
• Administració.

La protecció haurà d'abastar també els equips de comunicacions (*encaminadors, switches*, etc.). És recomanable seguir les pautes recollides en les guies CCN per a reforçar la seguretat d'aquests elements.

N/SEG/TEC-006-2 CONFIDENCIALITAT, AUTENTICITAT I INTEGRITAT EN LES COMUNICACIONS

Abans d'intercanviar qualsevol informació s'assegurarà l'autenticitat de l'altre extrem d'un canal de comunicació, tal com s'estableix en l'apartat N/SEG/TEC-004.

Es disposarà de mecanismes per a la prevenció d'atacs actius, i es garantirà que almenys siguen detectats i, en cas d'ocórrer, la consegüent activació dels procediments previstos de tractament de l'incident. Es consideren atacs actius aquells atacs en els quals s'altere la informació transmesa, s'inserisca informació enganyosa, o se segreste la comunicació per una tercera part.

Las comunicacions que discórreguen per xarxes fora del propi domini de seguretat, en aquells sistemes de categoria MITJANA i superior, utilitzaran xarxes privades virtuals (VPN), i empraran protocols estàndard com IPSEC o TLS. Els equips sense fils porten incorporat mecanismes de xifratge de les comunicacions, per la qual cosa hauran de ser configurats de manera segura emprant mecanismes actualitzats. En qualsevol cas, s'implementarà la criptologia corresponent en les comunicacions tal com marque la guia CCN-STIC 807.

Cal atendre el secret de les claus de xifra segons l'indicat en N/SEG/TEC-014-3. En el cas de xarxes privades virtuals, el secret ha de ser impredictible, mantindre's sota custòdia mentre dure la sessió i ser destruït en acabar. En el cas d'altres procediments de xifratge, cal tindre cura de les claus de xifra durant el seu cicle de vida en els termes recollits en l'apartat N/SEG/TEC-014-3.

Quan es tracte de sistemes crítics o de categoria ALTA s'empraran, preferentment, dispositius *hardware* en l'establiment i la utilització de la xarxa

privada virtual, de manera que les tasques de xifratge en els extrems es realitzen en els equips de *hardware* especialitzat, i s'evite el xifratge per programari. Els productes utilitzats hauran d'estar certificats conforme al que s'estableix en l'apartat N/SEG/TEC-021-3.

D'igual forma, quan es tracte de sistemes de categoria ALTA es durà a terme la segregació de xarxes. S'ha de segmentar la xarxa de manera que hi haja:

- Control (d'entrada) dels usuaris que poden treballar en cada segment, en particular si l'accés es fa des de l'exterior del segment, tant si és des d'un altre segment de la xarxa corporativa com si l'accés procedeix de l'exterior de la xarxa, tot extremant les precaucions en aquest últim escenari.
- Control (d'eixida) de la informació disponible en cada segment.
- Control (d'entrada) de les aplicacions utilitzables en cada segment.
- El punt d'interconnexió ha d'estar particularment assegurat, mantingut i monitorat.

No s'hauria de permetre cap protocol directe entre els segments interns i l'exterior, intermediant-hi tots els intercanvis d'informació.

Les xarxes es poden segmentar per dispositius físics o lògics.

N/SEG/TEC-007 OPERACIÓ DEL SISTEMA

La descripció detallada de com procedir a les tasques d'operació i explotació del sistema es recollirà en els procediments de treball corresponents. Aquests procediments respectaran, en qualsevol cas, el que es disposa en aquest apartat.

N/SEG/TEC-007-1 CONFIGURACIÓ DE SEGURETAT PER DEFECTE

S'haurà de realitzar una fortificació o reforçament del sistema d'informació previ a la seua entrada en operació de manera que s'implemente una configuració segura per defecte; per això hauran de seguir-se les guies CCN-STIC corresponents, mantenir la regla de "funcionalitat mínima" i "mínim privilegi", i cobrir almenys els aspectes següents:

a) Es retiraran els comptes i les contrasenyes estàndard.

b) Es desactivaran les funcionalitats tècniques no requerides, ni necessàries, ni d'interés o inadequades, ja siguen gratuïtes, d'operació, administració o auditoria. Aquestes funcionalitats quedaran documentades i constarà el motiu pel qual s'hagen deshabilitat.

c) Les funcions d'operació, administració i registre d'activitat seran les mínimes necessàries, i s'assegurarà que només són accessibles per les persones, o des d'emplaçaments o equips, autoritzats, i es podran exigir, si s'escau, restriccions d'horari i punts d'accés facultats.

d) Disposarà de mecanismes que garantisquen la correcció de l'hora a la qual es realitza el registre (d'activitat, d'incidències, etc.).

e) La configuració de seguretat només podrà editar-se per personal degudament autoritzat.

f) Existiran configuracions maquinari/programari, autoritzades i mantingudes regularment, per als servidors, elements de xarxa i estacions de treball.

g) Es verificarà periòdicament la configuració maquinari/programari del sistema per a assegurar que no s'han introduït ni instal·lat elements no autoritzats.

h) Es mantindrà una llista de serveis autoritzats per a servidors i estacions de treball.

i) S'establiran bloquejos de sessió per temps d'inactivitat, i es requerirà una nova autenticació de l'usuari per a reprendre l'activitat en curs.

j) S'habilitaran mecanismes de prevenció i reacció contra codi nociu (virus, cucs, troians, programes espia i programari maliciós en general) per a tots els equips (servidors i llocs de treball). Les opcions de configuració seran les recomanades pel fabricant, com també les referents a la freqüència d'actualització; en cas contrari, estarà documentat el motiu.

k) S'instal·larà programari de protecció contra codi nociu en tots els equips: llocs d'usuari, servidors i elements perimetrals.

l) Tot fitxer procedent de fonts externes serà analitzat abans de treballar amb ell.

m) Les bases de dades de detecció de codi nociu romandran permanentment actualitzades.

n) Tot el sistema s'escanejarà regularment per a detectar-hi codi nociu.

o) Les funcions crítiques s'analitzaran en arrancar el sistema en prevenció de modificacions no autoritzades.

p) El programari de detecció de codi nociu instal·lat en els llocs d'usuari haurà d'estar configurat de manera adequada i implementarà protecció en temps real, d'acord amb les recomanacions del fabricant.

q) L'ús ordinari del sistema pels usuaris haurà de ser senzill i segur. En cas d'haver-hi situacions que puguen posar en risc la seguretat, i sempre que es tracte de supòsits en què l'organització la consenta sota la responsabilitat de l'usuari, el sistema indicarà aquesta possibilitat i les conseqüències a l'usuari, de manera que aquest siga conscient de la seua exposició a un risc, i l'usuari haurà de donar el seu consentiment exprés, i assumir el risc. D'aquests consentiments informats dels usuaris quedarà constància en un registre.

Es disposarà d'un procediment documentat que indique la freqüència i els motius pels quals s'ha de modificar la configuració del sistema, i inclourà: l'aprovació del responsable, la documentació del canvi, les proves de seguretat del sistema sota la nova configuració i la retenció de la configuració prèvia per un temps preestablit.

N/SEG/TEC-007-2 DIMENSIONAMENT/GESTIÓ DE CAPACITATS

En aquells sistemes la dimensió de disponibilitat dels quals siga de nivell MITJÀ o superior, amb caràcter previ a l'adquisició o posada en explotació de qualsevol dels seus elements, es portarà a terme un estudi previ que cobrirà els aspectes següents:

a) Necessitats de processament.
b) Necessitats d'emmagatzematge d'informació: Durant el seu processament i durant el període que haja de retindre's.
c) Necessitats de comunicació.
d) Necessitats de personal: Quantitat i qualificació professional.
e) Necessitats d'instal·lacions i mitjans auxiliars.

f) Es farà una previsió de la capacitat i es mantindrà actualitzada durant tot el cicle de vida del sistema.
g) S'empraran eines i recursos per al monitoratge de la capacitat.

N/SEG/TEC-007-3 INTEGRITAT I ACTUALITZACIÓ DEL SISTEMA

Es disposarà d'un pla de manteniment de l'equipament físic i lògic que indique la freqüència, els components a revisar, el responsable de la revisió i les evidències a generar. Respecte a aquest pla de manteniment:

- Atendrà les especificacions dels fabricants quant a instal·lació i manteniment dels sistemes.

- Contemplarà mecanismes per al seguiment continu dels anuncis de defectes i un procediment documentat que indique qui i amb quina freqüència ha de monitorar aquests anuncis, així com el procediment per a analitzar, prioritzar i determinar quan aplicar les actualitzacions de seguretat, pegats, millores i noves versions.

- El manteniment només el podrà efectuar personal degudament autoritzat.

N/SEG/TEC-007-4 GESTIÓ DE CANVIS

Haurà de mantindre's un control continu de canvis realitzats en el sistema. En aquest sentit, es comptarà amb un procediment de gestió de canvis que indicarà la freqüència i els motius pels quals s'ha de canviar un component del sistema i inclourà: l'aprovació del responsable, la documentació del canvi, les proves de seguretat del sistema després del canvi i la retenció d'una còpia del component previ per un temps preestablit.

Respecte a aquest control de canvis:

- Analitzarà tots els canvis anunciats pel fabricant o proveïdor per a determinar la seua conveniència per a ser incorporats o no.

- Els canvis es planificaran per a reduir l'impacte sobre la prestació dels serveis afectats. Per això, totes les peticions de canvi es registraran i se'ls assignarà un número de referència que en permeta el seguiment, de manera equivalent al registre dels incidents.

- La informació a registrar per a cada petició de canvi serà suficient perquè qui haja d'autoritzar-lo no tinga dubtes sobre aquest tema i permeta gestionar-lo fins a la seua desestimació o implementació.

- Abans de posar en producció una nova versió o una versió apedaçada es comprovarà en un equip que no estiga en producció (equivalent al de producció en els aspectes que es comproven) que la nova instal·lació funciona correctament i no disminueix l'eficàcia de les funcions necessàries per al treball diari. L'equip de proves serà equivalent al de producció en els aspectes que es comproven.

- Les proves de preproducció, sempre que siga possible realitzar-les, s'efectuaran en equips equivalents als de producció, almenys en els aspectes específics del canvi.

• Una vegada implementat el canvi, es realitzaran les proves d'acceptació convenients. Si són positives, s'actualitzarà la documentació de configuració (diagrames de xarxa, manuals, inventari, etc.), sempre que procedisca.

• Es planificaran els canvis per a reduir l'impacte sobre la prestació dels serveis afectats.

• Es determinarà, mitjançant anàlisi de riscos, si els canvis són rellevants per a la seguretat del sistema. En cas que el canvi implique una situació de risc de nivell alt haurà de ser aprovat explícitament de manera prèvia a la seua implantació.

N/SEG/TEC-007-5 OPERACIÓ D'EINES DE SEGURETAT

En general, es consideraran eines de seguretat el conjunt de *maquinari* o *programari* que proporcionen serveis orientats a reforçar i donar suport a la seguretat dels sistemes.

Les eines de seguretat es classificaran, sobre la base de la seua funcionalitat principal, en les categories següents:

a. Auditoria
b. Prevenció
c. Detecció
d. Resposta
e. Conservació

Les eines de seguretat podran operar a diferents nivells (xarxa, sistema, usuari, aplicació) o ser una combinació de tots ells (multinivell).

a) **Eines d'auditoria**. Són aquelles eines l'objectiu de les quals és l'anàlisi de l'estat en matèria de seguretat dels sistemes en un moment determinat. Entraran en aquesta categoria eines com els escàners de xarxa, les de revisió de la configuració, les d'auditoria de contrasenyes i de codi, les d'anàlisis de metadades i de vulnerabilitats.

b) **Eines de prevenció**. Entraran en aquesta categoria eines com els dispositius de protecció perimetral (encaminadors, tallafocs, *proxys*), de detecció i prevenció d'intrusions, de neteja de metadades, de gestió de contrasenyes, antivirus i filtres *anti spam*.

c) **Eines de detecció**. Entraran en aquesta categoria eines com les de captura, monitoratge i anàlisi de trànsit de xarxa, les de monitoratge i supervisió de dispositius de xarxa, o les de monitoratge i anàlisi de registres del sistema.

d) **Eines de resposta**. Entraran en aquesta categoria eines com les d'anàlisis de codi nociu, les de gestió d'incidències.

e) **Eines de conservació.** Entraran en aquesta categoria eines com les d'anàlisi forense i les de còpia de seguretat.

Qualsevol eina de seguretat que pretenga incorporar-se als sistemes d'informació haurà de ser autoritzada prèviament pel responsable de Seguretat dels Sistemes d'Informació, després de comprovar la idoneïtat de l'eina per a l'objectiu pretés, el seu ajust als paràmetres legals i de qualitat i als requisits determinats en la present norma.

Sense perjudici del que s'estableix en l'apartat N/SEG/TEC-001-2, haurà d'existir un inventari i registre de les eines de seguretat on conste els qui estan autoritzats per a la instal·lació i desinstal·lació, configuració, modificació, manteniment i operació, com també l'accés a la informació que, si s'escau, pogueren generar.

A l'hora d'aplicar canvis en la configuració d'aquestes eines, requerits per actualitzacions del proveïdor, s'haurà de tindre en compte la necessitat o no de noves funcionalitats i, en qualsevol cas, s'haurà d'acordar amb el responsable de Seguretat dels Sistemes d'Informació la idoneïtat del canvi en la configuració, ja que es deu a una situació creada pel proveïdor i no per una necessitat de l'organisme i que, per tant, no té per què derivar en un canvi. En cas que es faça el canvi, s'han de documentar els requisits d'actualització i la motivació d'aquesta.

L'operació d'aquestes eines s'ajustarà al que s'estableix en els procediments d'operació del sistema que se citen a l'inici d'aquesta norma. No obstant això, en qualsevol cas, aquests procediments hauran d'abordar, com a mínim, els aspectes següents:

• Control de la configuració i gestió de l'eina: Definint rols i perfils a implementar, a fi de garantir que els usuaris tenen el nivell d'accés adequat a la seua tasca i responsabilitat.

• Anàlisi i protecció de dades: S'haurà d'indicar com manejar les dades que s'obtinguen a partir de l'operació de l'eina, així com les maneres de protegir-les davant de modificació, revelació, destrucció, etc., no autoritzades.

• Definició d'operació bàsica, la qual ha de cobrir la major part del dia a dia de l'operació de l'eina.

• Gestió d'incidents derivats de l'ús de l'eina, i indicar les persones que han de ser informades i que estaran identificades en aquests procediments.

La documentació generada per les eines de seguretat s'haurà de qualificar conforme al que s'estableix en la norma N/SEG/USU-001-1, en virtut de la qual s'aplicaran les mesures pertinents per a la seua protecció i distribució.

N/SEG/TEC-008 *PROGRAMARI DE GESTIÓ*

N/SEG/TEC-008-1 INSTAL·LACIÓ I ÚS

Els usuaris no hauran d'instal·lar cap mena de programari, ni tan sols còpies del programari propietat de la corporació, per iniciativa pròpia. Únicament en casos degudament justificats, i sota les garanties de seguretat corresponents, podrà autoritzar-se la instal·lació de determinat programari per part dels usuaris mateixos.

Qualsevol necessitat de programari o d'aplicació serà canalitzada a través del Servei d'Informàtica mitjançant el procediment habitual de peticionés d'equipaments i serveis, i s'indicarà també la finalitat de la petició. La petició, en qualsevol cas, haurà de comptar amb la validació del màxim responsable tècnic del servei o la unitat al qual pertanga el peticionari.

Tota sol·licitud serà objecte de l'anàlisi i valoració corresponents en el Servei d'Informàtica, amb la finalitat d'adequar-la als recursos estàndard de la Diputació de València i implantar, si s'escau, una alternativa òptima. La valoració haurà de tindre en compte els requisits següents:

• Si hi ha un programari amb les mateixes o similars característiques ja instal·lat a l'entorn de l'organització. No es produiran adquisicions ni instal·lacions de programes les funcionalitats dels quals puguen ser similars a un programari preexistent.

• Si el programari sol·licitat és per a tractar dades de caràcter personal haurà de proporcionar les garanties establides per a aquesta mena de tractaments. El producte especificarà en la seua descripció tècnica el nivell de seguretat que permet aconseguir.

• Es mantindrà actualitzada una relació formal del component programari de tercers empleats en el desplegament del sistema. Aquesta llista inclourà llibreries programari i els serveis requerits per al seu desplegament (plataforma o entorn operacional). El contingut de la llista de components serà equivalent al requerit en [mp.sw.1.r5] ENS.

• El programari complirà les garanties recollides en l'apartat N/SEG/TEC-008-3.

N/SEG/TEC-008-2 DESENVOLUPAMENT D'APLICACIONS

En el desenvolupament d'aplicacions es compliran els requisits següents:

- El desenvolupament haurà de realitzar-se sobre un sistema diferent i separat del de producció, i no haurà d'haver-hi eines o dades de desenvolupament a l'entorn de producció. L'inventari d'actius identificarà expressament els servidors utilitzats per a desenvolupament.

- S'aplicarà una metodologia de desenvolupament reconeguda que prenga en consideració els aspectes de seguretat al llarg de tot el cicle de vida,

tracte específicament les dades usades en proves i permeta la inspecció del codi font.

- Les aplicacions es desenvoluparan respectant el principi de mínim privilegi, i accediran únicament als recursos imprescindibles per a la seua funció, i amb els privilegis que siguen indispensables.

- Formaran part integral del disseny del sistema: Els mecanismes d'identificació i autenticació; els mecanismes de protecció de la informació tractada i la generació i tractament de pistes d'auditoria.
- S'aplicarà una metodologia de desenvolupament segur reconeguda que:

    (a) Tindrà en consideració els aspectes de seguretat al llarg de tot el cicle de vida.
    (b) Inclourà normes de programació segura, especialment: control d'assignació i alliberament de memòria, desbordament de memòria (overflow).
    (c) Tractarà específicament les dades usades en proves.
    (d) Permetrà la inspecció del codi font.

- Els elements següents seran part integral del disseny del sistema:
    (a) Els mecanismes d'identificació i autenticació.
    (b) Els mecanismes de protecció de la informació tractada.
    (c) La generació i tractament de pistes d'auditoria.

- Les proves anteriors a la implantació o modificació dels sistemes d'informació no s'efectuaran amb dades reals, llevat que s'assegure el nivell de seguretat corresponent i s'anote la seua realització en el document de seguretat si s'afecten dades de caràcter personal. Si està previst realitzar proves amb dades reals, prèviament s'haurà d'haver fet una còpia de seguretat.

N/SEG/TEC-008-3 ENTRADA EN PRODUCCIÓ

Abans de passar a producció es comprovarà el funcionament correcte de l'aplicació. Es comprovarà que es compleixen els criteris d'acceptació en matèria de seguretat i que no es deteriora la seguretat d'altres components del servei. Les proves es realitzaran en un entorn aïllat (preproducció) i no es portaran a terme amb dades reals, llevat que s'assegure el nivell de seguretat corresponent.

Quan es tracte d'aplicacions de sistemes d'informació de categoria MITJANA i superior, prèviament a l'entrada en servei es farà una anàlisi de vulnerabilitats que constarà de tres fases:

- Revisió exhaustiva dels components del programari, centrant-se en la seua superfície d'interacció amb els usuaris, amb serveis de suport i amb altres programes.
- Anàlisi de possibles vulnerabilitats en els elements identificats en el primer pas i estimació de l'impacte potencial que suposaria un incident.
- Proves de penetració per a cerciorar-se si la vulnerabilitat és utilitzable, prioritzant aquells punts de major impacte potencial. Han de fer-se proves simulant usuaris externs i usuaris interns, en funció dels qui siga accessible el programari.

Quan es tracte d'aplicacions de sistemes d'informació crítics o de categoria ALTA, a més, es farà una anàlisi de coherència en la integració en els processos i es considerarà l'oportunitat de realitzar una auditoria de codi font. L'anàlisi de coherència abastarà els processos administratius implicats, realitzarà proves comprovant que les dades d'entrada produeixen les dades d'eixida correctes i quines dades incorrectes d'entrada són detectades i atallades abans de destruir la integritat del sistema.

N/SEG/TEC-009 SEGURETAT EN ENTORNS I APLICACIONS WEB

La seguretat en el procés de disseny i desenvolupament d'una aplicació Web ha d'abordar principalment dos elements:

a) L'entorn de desenvolupament Web, en el qual s'haurà de disposar de l'última versió que soluciona vulnerabilitats de seguretat prèvies i conegudes.
b) L'aplicació Web propietària, codi propi, basada en el llenguatge de programació utilitzat.

Hauran de consultar-se de manera periòdica les bases de dades de vulnerabilitats per a estar al dia sobre els últims atacs, incidents i vulnerabilitats sobre entorns Web i el seu impacte. Es recomanen com a fonts d'informació detallada respecte a vulnerabilitats de seguretat CCN-CERT, *SecurityFocus* i SANS.

N/SEG/TEC-009-1 ESTRATÈGIA I METODOLOGIA

Els elements de seguretat principals d'un entorn o aplicació Web han d'incloure:

• Formació en seguretat d'aplicacions Web
• Arquitectura i infraestructura (sistemes i xarxes) segura
• Metodologia de seguretat de desenvolupament d'aplicacions Web
• Metodologia d'anàlisi de seguretat d'aplicacions Web

L'estratègia i metodologia de seguretat ha d'incloure addicionalment els components següents:

• Formació en seguretat.

• Instal·lació i configuració segura de sistemes i xarxes (arquitectura).
    - Actualitzacions: Servidor Web i d'aplicació, *framework*, etc.
• Desenvolupament de *programari* segur.
    - Gestió de versions i actualitzacions.
• *Web Application Firewalls* (WAF).
• Auditories de seguretat.
    - Caixa negra: Proves d'intrusió i *Web Application Security Scanners* (WASS).
    - Caixa blanca: Revisió de codi manual i automàtic.
• Resposta davant incidents.

N/SEG/TEC-009-2 ARQUITECTURES DE SEGURETAT EN ENTORNS WEB

S'utilitzaran preferentment models d'arquitectura d'aplicacions Web de tres capes (servidor Web, servidor d'aplicació i base de dades).

L'arquitectura de l'aplicació Web ha de disposar de mecanismes de detecció i protecció a nivell de xarxa, i inclourà elements de seguretat tradicionals com tallafocs o sistemes de detecció d'intrusos.

Serà necessari disposar de dispositius dedicats exclusivament a la inspecció i el filtrat del trànsit Web, és a dir, el protocol HTTP o HTTPS, ja que els tallafocs tradicionals no disposen de capacitats avançades per a analitzar i bloquejar els atacs rebuts a través d'aquest protocol.

En el cas que siga necessari assegurar la confidencialitat de les comunicacions Web s'hi farà ús de la versió segura del protocol (HTTPS).

Addicionalment als elements de seguretat propis d'un entorn Web, és necessari protegir tots els elements de la infraestructura en la qual resideix l'aplicació Web,

com ara dispositius de comunicacions (*encaminadors, switches*, etc.) o la infraestructura de servidors de noms (DNS-SEC).

Els mecanismes de protecció a implementar han de protegir els diferents equips contra:

• Atacs directes, com ara accessos no autoritzats sobre qualsevol dels elements que conformen l'entorn o aplicació Web.
• Atacs indirectes, en els quals qualsevol dels elements és emprat com a eina en l'atac.
• Atacs de denegació de servei (DoS).

S'hauran d'aplicar els últims pedaços de seguretat en cadascun dels elements de programari que formen part de la plataforma de l'aplicació Web: Programari dels dispositius de xarxa i tallafocs, sistema operatiu dels servidors (Web, aplicació i base de dades), i programari de la plataforma de desenvolupament emprada (PHP, ASP, Java, etc.).

N/SEG/TEC-009-3 DESENVOLUPAMENT SEGUR DEL *PROGRAMARI* D'APLICACIONS *WEB*

L'element fonamental en la metodologia de seguretat de desenvolupament de programari d'aplicacions Web passa per incloure tots els aspectes de seguretat en el cicle de vida de desenvolupament del programari (SDLC, *Software Development Life Cycle*).

Se seguiran les especificacions contingudes en la Guia CCN-STIC-812 pel que fa a les recomanacions generals, filtrat de dades d'entrada o accés de l'usuari, gestió de missatges d'error, autenticació i gestió de sessions, atacs CSRF, atacs de manipulació d'URL, atacs de manipulació d'informació emmagatzemada en disc, atacs a *cookies*, escalat de privilegis i gestió de *Logs*.

N/SEG/TEC-009-4 ANÀLISI DE SEGURETAT D'APLICACIONS WEB

L'objectiu de l'anàlisi de seguretat d'una aplicació Web és passar d'una aplicació Web que presenta vulnerabilitats a una aplicació que és segura i no té vulnerabilitats conegudes. La metodologia d'anàlisi ha d'incloure dues àrees:

- Caixa negra. L'anàlisi de caixa negra se centra en estudiar les vulnerabilitats de seguretat de l'aplicació Web des del punt de vista d'un atacant extern.
- Caixa blanca. L'anàlisi de caixa blanca se centra en estudiar les vulnerabilitats de seguretat de l'aplicació Web des del punt de vista del desenvolupador.

La freqüència d'aquestes auditories de seguretat quedarà definida en el procediment d'auditoria.

N/SEG/TEC-009-5 ADMINISTRACIÓ DE LA NAVEGACIÓ PER *INTERNET*

Per a poder administrar la navegació per internet s'hauran d'establir els paràmetres següents:

a) Els ports autoritzats. De manera que es predeterminen els diferents ports que es consideren autoritzats per a cada tipus de servei (http; https; sftp…)

b) Si s'escau, els diferents grups d'accés (tipus d'usuari d'internet) en funció de les categories de pàgines web.

c) El catàleg de tipus de fitxer d'accés restringit, per a minimitzar els riscos derivats de la descàrrega de fitxers.

d) La distribució dels diferents nivells d'usuaris atenent a:

- Les categories dels continguts per als quals tenen permís d'accés.
- Els tipus de fitxers que tenen permís de descàrrega.
- Limitació del temps de consulta.

Els paràmetres anteriors els establirà el Comité de Seguretat TIC i els documentaran per a la seua aplicació els responsables de l'administració de la navegació per internet.

Es protegirà la informació de resolució d'adreces web i d'establiment de connexions.

N/SEG/TEC-010 SEGURETAT EN ENTORNS *CLOUD*

En aquest apartat s'exclouen els possibles serveis de *Cloud Computing* que la Diputació de València poguera prestar a tercers, o a si mateixa, mitjançant la utilització d'actius interns (equips, locals, persones, programes).

N/SEG/TEC-010-1 TIPOLOGIA D'ENTORNS *CLOUD*

Als efectes exclusius de seguretat, es distingiran els següents tipus d'entorns *Cloud* externs —plataformes, programes o serveis que poden ser utilitzats per la Diputació com a part dels recursos (actius) per a prestar un servei i/o explotar una informació—:

A) Entorns els actius dels quals es troben sota el control i la gestió de la Diputació de València. Es tracta de plataformes, programes o serveis que es mantenen sota el seu domini de seguretat. S'hi apliquen directament les polítiques i normes de seguretat internes.

B) Entorns els actius dels quals es troben parcialment sota el control i la gestió de la Diputació de València. Normalment per tractar-se de serveis no integrals (IaaS, PaaS, CaaS, BaaS). S'hi aplicarà allò previst en l'apartat N/SEG/TEC-010-3.

C) Entorns els actius dels quals es troben sota el control i la gestió d'un tercer. El tercer pot ser:

   - Un ens públic. Resulta indiferent si la posada a disposició comporta algun tipus de contraprestació econòmica (taxa, etc.) o no, si els recursos són de total propietat de l'organisme públic corresponent o si es tracta d'una "posada en comú". S'aplicarà el que es preveu en l'apartat N/SEG/TEC-001-3.

- Un ens privat. Normalment proveïdors de serveis *Cloud* de tipus generalista (Dropbox, Google Drive, Box, iCloud…) o sota demanda; en aquest últim cas, per resultar proveïdors integrals (SaaS). S'hi aplicarà allò previst en l'apartat N/SEG/TEC-010-3.

N/SEG/TEC-010-2 AUTORITZACIÓ PER A L'ÚS D'ENTORNS *CLOUD*

La utilització de serveis *Cloud* requerirà en tots els casos l'autorització del Comité de Seguretat TIC. L'autorització podrà ser genèrica, i delimitarà clarament els supòsits que s'hi inclouen, sense marge d'interpretació. L'autorització haurà de valorar els elements següents:

a) Classificació de la informació implicada, segons el que es disposa en la norma N/SEG/USU-001-2
b) Normativa legal i interna d'aplicació
c) Garanties de seguretat oferides per l'entorn
d) Anàlisi de riscos
e) Alternatives tècniques o serveis similars
f) Opinió del responsable de Seguretat dels Sistemes d'Informació

L'autorització podrà quedar supeditada al compliment de determinades condicions i/o l'adopció d'unes certes mesures, i tot això haurà de figurar en aquesta autorització.

N/SEG/TEC-010-3 REQUISITS DE SEGURETAT

Els requisits de seguretat que resulten d'aplicació (N/SEG/TEC-001-1) no varien pel fet d'utilitzar serveis *Cloud* externs. Però els diferents nivells de prestació del servei (IaaS, PaaS, CaaS, BaaS, SaaS) i el model de desplegament (núvol públic, privat o híbrid) condicionen les obligacions de seguretat de les parts, per la qual cosa s'haurà d'establir en un document vinculant per al proveïdor del servei, amb caràcter general, sobre qui recauen aquestes responsabilitats.

No obstant això, atesa l'especialitat d'aquesta mena de serveis, se seguiran sempre les indicacions següents:

• Quan s'utilitzen serveis en el núvol subministrats per tercers, els sistemes d'informació que els suporten hauran de ser conformes amb l'ENS o complir amb les mesures desenvolupades en una guia CCN-STIC.

• Quan es tracte de serveis de simple allotjament d'informació, i llevat que aquesta informació estiga classificada com a PÚBLICA, totes les dades se xifraran abans d'eixir de l'àmbit de la Diputació, de manera que els requisits de seguretat sobre els proveïdors es redueixen a la dimensió de disponibilitat. L'organisme serà l'únic en poder de les claus de xifra, a les quals aplicarà el que es preveu en l'apartat N/SEG/TEC-014-2.

• En qualsevol cas, las claus de xifra no s'emmagatzemaran en clar en el núvol, ni s'utilitzaran en aplicacions que s'executen en el núvol.

• El procés d'autorització d'usuaris (altes, baixes i gestió de drets d'accés) no es realitzarà en el núvol.

• Les aplicacions de firma electrònica i de segells de temps no s'executaran en proveïdors de serveis *Cloud* de caràcter general, sinó amb els mitjans propis o de terceres parts de confiança, d'acord amb la legislació aplicable en la matèria.

• Els elements virtualitzats i els elements de virtualització es tractaran igual que els elements físics corresponents a l'efecte de configuració, manteniment, regles de seguretat i aspectes reguladors.

• Les imatges dels elements virtuals es tractaran com a dades amb els mateixos requisits de seguretat que la informació i els serveis manejats per aquests elements virtuals.

• Els components de seguretat del tipus DMZ, tallafocs o agents (proxy) no hauran de residir en la mateixa màquina base que els components de producció.

• Es registraran totes les actuacions de creació, trasllat, activació i destrucció d'elements virtuals. Així mateix, es registrarà el muntatge i la retirada de suports d'informació, físics o virtuals.

• Els requisits d'identificació i autenticació de l'administrador de l'hipervisor correspondran als d'un sistema de categoria MITJANA, segons l'Esquema Nacional de Seguretat.

• En el supòsit de sistemes de categoria MITJANA, a més de l'anterior:

- No es compartiran equips base amb altres comunitats d'usuaris.
- No es compartirà el mateix hipervisor amb altres comunitats d'usuaris.
- L'administració de l'hipervisor estarà separada de l'administració dels elements virtualitzats: Diferents interfícies, diferents comptes d'administrador i diferents administradors.
- Els requisits d'identificació i autenticació de l'administrador de l'hipervisor correspondran als d'un sistema de categoria ALTA segons l'Esquema Nacional de Seguretat.

• En el supòsit de sistemes de categoria ALTA, a més de l'anterior:

- La xarxa administrativa estarà separada lògicament (xarxa privada virtual) o físicament (xarxa específica) de la xarxa administrativa d'altres comunitats d'usuaris.

N/SEG/TEC-010-4 CONTRACTACIÓ DE SERVEIS *CLOUD*

Sense perjudici del que s'estableix en l'apartat N/SEG/TEC-021-2, la contractació de serveis de *Cloud Computing* es durà a terme tenint en compte el següent:

• Els serveis en el núvol es troben tipificats com a contractes de servei, d'acord amb l'article 10 de l Reial decret legislatiu 3/2011 pel qual s'aprova el Text Refós de la Llei de Contractes del Sector Públic.

• Aquests contractes hauran de reflectir almenys els aspectes següents:

- Descripció del servei.
- Tipus de servei (IaaS, PaaS, SaaS…).
- Tipus d'infraestructura (núvol públic, privat o híbrid).
- Capacitat del servei.
- Protecció de la informació.
- Acords de nivell de servei (nivells, temps de resposta, penalitzacions, etc.).
- Mecanismes d'accés al servei.
- Responsabilitats i obligacions.
- Requisits legals.
- Requisits per al compliment de l'ENS.
- Gestió de canvis.

- Registre d'activitat.
- Gestió d'incidents.
- Eliminació d'informació.
- Suport i recuperació de dades.
- Continuïtat del servei.
- Finalització del servei.
- Requisits per a la protecció de dades personals.

• Quan el proveïdor *Cloud* puga contractar un tercer com a suport dels seus serveis (personal, instal·lacions, serveis de comunicacions, serveis de còpies de seguretat…), aquestes subcontractacions hauran d'estar previstes en el contracte, com també fer constar que han de ser informades i acceptades per la Diputació de València. Les obligacions del proveïdor en matèria de seguretat es transmeten de manera transitiva a les parts subcontractades. En particular els nivells de seguretat de la informació a la qual tinga accés el proveïdor i dels serveis que d'aquest últim depenguen; per tant, haurà de fer-se constar també en el contracte.

• Quan s'utilitzen serveis en el núvol subministrats per tercers, aquests hauran d'estar certificats sota una metodologia de certificació reconeguda per l'Organisme de Certificació de l'Esquema Nacional d'Avaluació i Certificació de Seguretat de les Tecnologies de la Informació. Si el servei en el núvol és un servei de seguretat haurà de complir amb els requisits establits en [op.pl.5].

• El contracte podrà imposar condicions sobre la ubicació geogràfica dels servidors i/o de les línies de comunicacions en funció de la informació que hagen d'acollir o transportar, respectivament. Aquestes condicions típicament deriven de requisits del propietari de la informació com, per exemple, per raons horàries i de majors facilitats per a exercir els controls i les auditories definides, o de condicionants legals respecte de la informació (per exemple, en dades de

caràcter personal), i permetrà identificar el marc legal aplicable, garantir en major mesura el seu compliment i reduir els riscos associats.

• El contracte definirà els rols de les persones involucrades en la prestació del servei, tant en la part de la Diputació com del proveïdor del servei *Cloud*. S'han de considerar les següents responsabilitats mínimes. En tractar-se de procediments de coordinació, les dues parts han de definir els seus interlocutors relatius:

- Responsable de la seguretat
- Persona de contacte per a incidents de seguretat
- Persona de contacte per a canvis i manteniment de sistemes
- Persona de contacte per a incidències relatives als indicadors de servei (SLA)
- Persona de contacte per a aspectes contractuals
- Persona de contacte per a temes jurídics i reguladors, en particular quant a dades de caràcter personal

• Els requisits de seguretat en aquests contractes han d'establir-se concordes amb la Declaració d'Aplicabilitat que corresponga i amb el resultat de l'anàlisi de riscos, per la qual cosa hauran de ser prèviament recaptats del responsable de Seguretat dels Sistemes d'Informació.

• És necessari identificar en el contracte els drets de la Diputació per a poder monitorar el funcionament del servei i d'aquesta manera poder comprovar el compliment de les mesures de seguretat, els controls i les polítiques que garanteixen la integritat, confidencialitat i disponibilitat de les dades, i de la mateixa manera poder realitzar la comprovació que el nivell de prestació és el pactat. La Diputació haurà de reservar-se sempre la potestat d'auditoria respecte dels actius sota el control i la gestió del proveïdor de serveis, inclosos els

possibles subcontractistes, a l'efecte de comprovar de primera mà el compliment dels requisits contractuals.

• La finalització del servei haurà d'estar recollida en la descripció del servei mateix, identificant la necessitat que puga haver-hi que el proveïdor retorne la informació a la finalització de la relació contractual i fent constar això en una clàusula al costat del temps que tardarà el proveïdor a realitzar la migració de les dades. Referent a això, es buscarà la "neutralitat tecnològica" del servei que facilite tot tipus de retorn o migració.

N/SEG/TEC-011 SEGURETAT EN DISPOSITIUS PORTÀTILS I MÒBILS

Sense perjudici d'allò disposat en aquest apartat, se seguiran les pautes recollides en les guies CCN següents per a reforçar la seguretat d'aquests dispositius:

· CCN-STIC-827 Gestió i ús de dispositius mòbils
· CCN-STIC-45X Seguretat de dispositius mòbils

S'haurà d'elaborar un procediment que contemple les directrius de posada en operació, entrega i baixa dels dispositius portàtils i mòbils.

Els equips (ordinadors portàtils, tauletes, etc.) que siguen susceptibles d'eixir de les instal·lacions de l'organització i no puguen beneficiar-se de la protecció física corresponent, amb un risc manifest de pèrdua o robatori, seran protegits adequadament.

N/SEG/TEC-011-1 SEGURETAT PER DEFECTE

La configuració de la seguretat per defecte a la qual es refereix la norma N/SEG/USU-002-3 atendrà els principis bàsics següents:

• La limitació o restricció de la connexió directa a xarxes externes, dels canals, ports i sistemes de comunicacions d'eixida d'informació, de la instal·lació i execució de programari i dels serveis que seran accedits, serà establida pel Comité de Seguretat TIC, atesos els riscos que per a la seguretat siguen presents en funció del tipus de dispositiu, el perfil d'usuaris, la naturalesa de la informació a tractar i l'entorn d'utilització.

• Es portarà un inventari de dispositius portàtils, juntament amb una identificació de la persona responsable de cadascun d'aquests i un control regular que està positivament sota el seu control.

• S'establirà un procediment operatiu de seguretat per a informar el servei de gestió d'incidents de pèrdues o sostraccions.

• Quan un dispositiu portàtil es connecte remotament a través de xarxes que no estan sota el control estricte de l'organització, l'àmbit d'operació del servidor limitarà la informació i els serveis accessibles als mínims imprescindibles, i requerirà autorització prèvia dels responsables de la informació i els serveis afectats. Aquest punt és aplicable a connexions a través d'internet i altres xarxes que no siguen de confiança.

• S'evitarà, en la mesura que siga possible, que els dispositius continguen claus d'accés remot a l'organització. Es consideraran claus d'accés remot aquelles que siguen capaços d'habilitar un accés a altres equips de l'organització, o altres de naturalesa anàloga.

• En cas que siga necessari emmagatzemar claus en aquests dispositius, aquestes estaran, al seu torn, xifrades per altres claus que només el propietari del maquinari que les té emmagatzemades siga capaç de generar i utilitzar.

• S'implantaran solucions de gestió centralitzada dels dispositius, del tipus MDM (*Mobile Device Manegement*) o similar, que permeten, en qualsevol cas, el monitoratge, l'esborrament remot de dades o la realització d'auditories de seguretat sobre aquests dispositius.

• Es procurarà l'entrega dels dispositius amb un filtre de privacitat integrat en el monitor o la pantalla, de manera que es protegisca de la visió de tercers.

• Per al xifratge dels dispositius es recorrerà a les utilitats més indicades, siguen del sistema operatiu mateix, de la plataforma de gestió o altres solucions específiques.

N/SEG/TEC-011-2 DISPOSITIUS PORTÀTILS

Es preferiran els ordinadors portàtils en els quals l'accés a la BIOS puga estar protegit mitjançant un accés amb PIN/contrasenya, únicament conegut pels configuradors d'aquests dispositius del Servei d'Informàtica i Organització.

En tot cas, per als portàtils és aconsellable utilitzar un sistema de xifratge en *pre-boot*, que demane una contrasenya d'accés i desxifratge del disc dur.

N/SEG/TEC-011-3 DISPOSITIUS MÒBILS

Es preferiran sistemes operatius amb menor incidència contrastada de *malware*.

En el cas de sistemes operatius en els quals siga factible que l'usuari puga disposar dels màxims privilegis administratius sobre el dispositiu mòbil i puga prendre control complet del terminal (*jailbreak o rooting)*, les solucions MDM adoptades hauran de comptar amb capacitats de detecció per a identificar si un dispositiu ha patit aquest tipus de processos i notificar sobre aquesta situació a l'administrador de seguretat.

Les solucions MDM adoptades disposaran, en qualsevol cas, de les funcionalitats de gestió següents:

- Restriccions de programari i maquinari
- Codi d'accés
- Protecció remota
- Gestió i esborrament de dades remot
- Serveis de localització
- Certificats digitals
- Comunicacions (*Wifi, Bluetooth*, etc.)
- VPN
- Correu electrònic
- Navegació web
- APP

En el cas de dispositius aportats pels usuaris mateixos, si per qualsevol raó tècnica no poguera garantir-se la seguretat o la incomunicabilitat entre l'àrea professional i la privada, de manera que quede salvaguardat el dret a la privacitat, es denegarà la possibilitat d'ús del dispositiu en qüestió.

N/SEG/TEC-011-4 ALTRES DISPOSITIUS CONNECTATS A LA XARXA

Aquesta mesura afecta a tota mena de dispositius connectats a la xarxa i que puguen tindre en algun moment accés a la informació, com ara:

a) Dispositius multifunció: impressores, escàners, etc.
b) Dispositius multimèdia: projectors, altaveus intel·ligents, etc.
c) Dispositius internet de les coses, en anglés *Internet of Things* (IoT).
d) Dispositius de convidats i els personals dels empleats mateixos, en anglés *Bring Your Own Device* (BYOD).
e) Uns altres.

Els dispositius presents en el sistema hauran de comptar amb una configuració de seguretat adequada, de manera que es garantisca el control del flux definit d'entrada i eixida de la informació.

Els dispositius presents en la xarxa que disposen d'alguna mena d'emmagatzematge temporal o permanent d'informació proporcionaran la funcionalitat necessària per a eliminar informació de suports d'informació. (Vegeu [mp.si.5]).

S'usaran, quan siga possible, productes o serveis que complisquen el que s'estableix en [op.pl.5].

N/SEG/TEC-012 SIGNATURA ELECTRÒNICA I SEGELLAT DE TEMPS

La utilització de firma electrònica requerirà una **Política de Firma Electrònica i de Certificats**, aprovada per l'òrgan superior competent que corresponga, on constarà el conjunt de normes de seguretat, d'organització, tècniques i legals per a determinar com es generen, verifiquen i gestionen signatures electròniques, incloses les característiques exigibles als certificats de firma, els certificats, els serveis de segellament de temps i uns altres elements de suport de les firmes. Aquesta Política haurà de complir els requisits de l'Esquema Nacional d'Interoperabilitat.

Els sistemes podran utilitzar qualsevol mitjà de firma electrònica dels reconeguts per la legislació vigent. En aquest sentit, els protocols de firma electrònica faran ús de certificats digitals reconeguts. No s'admetrà l'ús de certificats la funció resum dels quals (*hash*) siga la funció MD5 o una altra de seguretat inferior.

Els sistemes d'informació de categoria MITJANA, a més:

- Quan s'empren sistemes de firma electrònica avançada basats en certificats, aquests seran qualificats.

- S'empraran algorismes i paràmetres autoritzats pel CCN o per un esquema nacional o europeu que resulte d'aplicació. El CCN determinarà els algorismes criptogràfics que hagen sigut autoritzats nominalment per al seu ús en l'Esquema Nacional de Seguretat, conforme a la Instrucció Tècnica de Seguretat Criptologia d'ocupació en l'ENS.

- Quan siga procedent, es garantirà la verificació i validació de la signatura electrònica durant el temps requerit per l'activitat administrativa que aquella suporte, sense perjudici que es puga ampliar aquest període d'acord amb el que establisca la Política de Firma Electrònica i de

Certificats que siga aplicable. Per a tal fi, a la firma s'adjuntarà, o es referenciarà, tota la informació pertinent per a la seua verificació i validació, inclosos certificats o dades de verificació i validació.

- Les signatures es protegiran amb segells de temps

Els sistemes d'informació crítics i els de categoria ALTA, a més:

- Utilitzaran dispositius segurs de creació de firma
- Empraran, preferentment, productes certificats

Sense perjudici del que puga establir la Política de Firma, en els sistemes de categoria ALTA caldrà complir amb:

• Els segells de temps previndran la possibilitat del repudi posterior.

• Els segells de temps s'aplicaran a aquella informació que siga susceptible de ser utilitzada com a evidència electrònica en el futur. En tot cas, es dataran electrònicament els documents la data i l'hora d'entrada dels quals i/o d'eixida s'haja d'acreditar fefaentment.

• Es dataran electrònicament les firmes la validesa de les quals haja d'estendre's per llargs períodes o així ho exigisca la normativa aplicable; alternativament es poden utilitzar formats de firma avançada que incloguen datació.

• Les dades pertinents per a la verificació posterior de la data seran tractades amb la mateixa seguretat que la informació datada a l'efecte de disponibilitat, integritat i confidencialitat.

• Es renovaran regularment els segells de temps fins que la informació protegida ja no siga requerida pel procés administratiu al qual dona suport.

• S'empraran "segells qualificats de temps electrònics" atenent el que es disposa en el Reglament (UE) núm. 910/2014 i normativa de desenvolupament.

• S'utilitzaran productes certificats o serveis externs admesos.

• En els sistemes crítics i de categoria ALTA es farà ús de sistemes de segellament de temps que utilitzen una Autoritat de Segellament de Temps (TSA), sent dels denominats esquemes simples o esquemes enllaçats.

N/SEG/TEC-013 SEGURETAT DEL CORREU ELECTRÒNIC

N/SEG/TEC-013-1 EINA DE CORREU SEGUR

S'haurà de realitzar una anàlisi dels riscos associats a l'ús del correu electrònic, sobre la base de la qual es determinaran les condicions que ha de complir l'eina utilitzada per a la seua gestió. Sense perjudici del que resulte de la citada anàlisi s'hauran de tindre en compte els factors següents:

a) Xifratge. El sistema ha de proporcionar xifratge robust i basat en estàndards internacionals.

b) Trànsit de dades. Si en la solució es produeix trànsit de dades en text clar, és necessari garantir que aquest trànsit no afecta la confidencialitat de la informació corporativa i que es compleixen les restriccions legals d'aplicació, especialment les relatives a dades de caràcter personal.

c) Costos. La implantació d'un sistema de correu segur determinat pot suposar un cert cost —tant directe com indirecte—, per la qual cosa és necessari analitzar en termes econòmics diferents alternatives i aplicar la més adequada en cada cas. El factor cost no s'ha d'anteposar de cap manera al factor seguretat.

d) Facilitat d'ús. La solució implantada ha de ser senzilla en el seu ús diari, almenys de manera relativa.

e) Capacitat d'integració. La solució a implantar ha d'integrar-se tot el possible tant amb les arquitectures (xarxa, *maquinari*, *programari*…) existents en l'organització com amb l'usuari, les seues capacitats i les seues necessitats.

f) Monitoratge. La solució triada, bé de manera directa bé a través de mecanismes indirectes, ha de generar els registres corresponents i disposar de capacitat d'alerta davant situacions anòmales que puguen repercutir en la seguretat de la informació corporativa (intents d'accés no autoritzats, funcionaments incorrectes, anomalies en l'ús del sistema…)

N/SEG/TEC-013-2 SEGURETAT DEL SERVIDOR DE CORREU

El servidor de correu electrònic corporatiu haurà d'estar situat en una zona desmilitaritzada (DMZ), i ha d'estar aïllat tant d'Internet com de la xarxa interna de l'organització mitjançant un tallafocs correctament configurat, que permeta únicament els trànsits estrictament necessaris per al funcionament correcte dels sistemes i serveis corporatius.

En qualsevol cas, el tallafocs o els tallafocs corporatius hauran de controlar el trànsit que es permet cap als sistemes de correu, tant des dels equips interns a l'organització com des dels equips situats en Internet.

Addicionalment a les regles anteriors, la Corporació, a través del Comité de Seguretat TIC, avaluarà la conveniència de denegar en el tallafocs corporatiu tot el trànsit SMTP sortint cap a Internet, amb excepció del generat en els servidors de correu electrònic, a fi d'evitar, entre altres, propagacions massives de *malware* des d'equips d'usuaris, ús d'equips interns per a realitzar atacs de *phishing*, etc.

Almenys, en els sistemes de categoria ALTA s'hauran d'implantar, en l'arquitectura sistemes de detecció o prevenció d'intrusions basats en xarxa (NIDS/NIPS) que permeten identificar o fins i tot detindre atacs o trànsits anòmals contra la plataforma de correu corporatiu; els registres generats per aquests entorns han de ser correctament analitzats per a garantir que s'emprenen les accions adequades davant una possible violació de la seguretat.

De la mateixa forma que la resta de sistemes corporatius, és crític que els servidors de correu estiguen correctament fortificats a nivell de sistema operatiu. Per això se seguiran les guies CCN-STIC corresponents a cada sistema concret, i s'aplicaran en aquest les directrius que marquen aquests documents.

El servidor o servidors de correu corporatiu han d'estar en sistemes dedicats, no compartint la seua funcionalitat amb altres entorns de l'organització per a evitar que vulnerabilitats en aquells afecten el correu electrònic. El programari instal·lat en el servidor ha de ser mínim, i eliminar aplicacions no estrictament necessàries per al funcionament del sistema de correu (eines ofimàtiques, entorns de desenvolupament, etc.).

En termes generals, s'hauran de considerar sempre els extrems següents:

a) Aplicació de pedaços i actualitzacions de seguretat en el sistema tan prompte com siga possible.

b) Eliminació dels serveis no necessaris per al funcionament correcte del sistema.

c) Restriccions d'accés adequades, tant des de la xarxa interna com des d'internet.

d) Polítiques de gestió d'usuaris i contrasenyes robustes.

e) Permisos correctes en tot el sistema d'arxius, prestant especial atenció a les carpetes de correu dels usuaris.

f) Monitoratge i control de paràmetres que impliquen anomalies en la seguretat.

N/SEG/TEC-013-3 SEGURETAT DELS SERVEIS DE CORREU

Els serveis associats al correu electrònic també s'han de configurar de manera segura. És especialment important garantir, en primer lloc, que les versions de les diferents aplicacions utilitzades per a la gestió del correu en el servidor siguen correctes tant des del punt de vista funcional com des del punt de vista de seguretat, tot aplicant les actualitzacions proporcionades pel fabricant sempre que siga necessari. En segon lloc, és necessari garantir que la configuració d'aquestes aplicacions és correcta també des dels dos punts de vista, ja que aplicacions actualitzades convenientment, però amb una deficient configuració, són susceptibles de ser atacades amb èxit per un tercer.

Cal limitar l'accés als serveis d'accés al correu electrònic a aquells orígens des dels quals efectivament siga necessari accedir a la gestió dels missatges per part dels usuaris. En cas que siga necessari l'accés a serveis d'enviament de correu des d'Internet , s'haurà de garantir el temps que el servidor de correu no actua

com a *open relay*, és a dir, no permet ser utilitzat per a l'enviament de correu no desitjat.

En el cas particular que es requerisca accés web al correu corporatiu s'ha de garantir la impossibilitat d'accedir a l'entorn evitant-ne l'autenticació. De la mateixa manera, ha de garantir-se que els atacs via web més habituals (XSS, SQL-i, LFI, RFI…) no afecten la seguretat del servei o l'aplicació web, bé mitjançant la implantació de sistemes de prevenció d'intrusions que detecten i aturen els atacs abans d'arribar al servidor, bé mitjançant una fortificació correcta de l'entorn web que proporciona correu electrònic a l'organització. Independentment del lloc on estiga permés l'accés via web al correu, el servidor web no ha d'estar situat en el mateix MTA (Agent de Transferència de Correu, situat en el servidor) corporatiu, sinó en un servidor independent a aquest, i la seua fortificació i auditoria han de ser correctes i completes en el temps. Totes les comunicacions entre el navegador —client— i el servidor web han d'estar obligatòriament xifrades, inclosa en primer lloc l'autenticació d'usuaris.

N/SEG/TEC-013-4 SEGURETAT DEL CLIENT DE CORREU

Per a garantir la seguretat del correu electrònic corporatiu, com a element clau en el flux de missatges, és necessari garantir la seguretat dels equips d'usuari utilitzats per a processar aquest correu. Per això, cal fortificar l'equip d'usuari de manera adequada, siga com siga el seu sistema operatiu, tenint en compte, sense menyscapte de qualssevol altres, els elements recollits en les guies de seguretat per a la configuració de servidors i de clients de correu.

Els clients de correu instal·lats en aquests equips han d'estar actualitzats permanentment a la seua última versió, almenys quant a pedaços de seguretat, com també correctament configurats.

N/SEG/TEC-013-5 SEGURETAT DEL CONTINGUT

Quan la informació continguda en el cos del missatge s'haja de protegir d'atacs d'intercepció, s'haurà de xifrar convenientment aquesta informació, bé mitjançant eines integrades en els clients de correu, bé mitjançant eines independents —en aquest cas s'adjuntarà l'arxiu xifrat com un fitxer més en el missatge—. Sempre que siga possible s'han de triar eines integrades amb els clients de correu corporatiu, de manera que s'hi facilite a l'usuari la gestió segura del seu correu des del client de correu mateix, sense necessitat d'eines externes.

Però qualsevol sistema de seguretat en el correu electrònic ha d'incorporar no sols el xifratge de la informació, sinó també la firma d'aquesta, sense importar el seu nivell de seguretat, de manera que el receptor, d'una banda, desxifre la informació i, d'una altra, gràcies a la firma digital, verifique que el receptor és qui diu ser i el contingut del correu és íntegre.

N/SEG/TEC-014 RECURSOS CRIPTOGRÀFICS

N/SEG/TEC-014-1 ÚS DE CRIPTOGRAFIA

Es durà a terme el xifratge de la informació sempre que es tracte de:

a) Aquella informació la dimensió de confidencialitat de la qual siga valorada de nivell alt.

b) Les dades de caràcter personal pertanyents a les categories especials de dades. En aquests casos caldrà usar el mecanisme d'encriptació fins i tot en les comunicacions de dades realitzades en l'àmbit intern de l'organització mateixa (xarxes locals).

c) Aquella informació que, com a resultat de l'anàlisi de riscos, així ho aconselle.

d) Qualssevol altres supòsits recollits expressament en la normativa interna de seguretat i protecció de dades personals.

En tots els casos s'ha de xifrar la informació tant durant el seu emmagatzematge com durant la seua transmissió. Només estarà en clar mentre se n'està fent ús. Això inclou:

- Xifratge de fitxers
- Xifratge de directoris
- Discos virtuals xifrats
- Xifratge de dades en bases de dades

Per al xifratge d'informació, ja siga en trànsit o mentre estiga emmagatzemada, s'utilitzaran sistemes de xifratge segurs, seguint el que s'estableix en l'apartat N/SEG/TEC-006-2 per al xifratge de les comunicacions. El Servei d'Informàtica aportarà les solucions tècniques necessàries per al xifratge de la informació.

Quan es reclamen productes certificats, s'entendrà per tal tots aquells que hagen sigut avaluats conforme a normes europees o internacionals i que estiguen certificats per entitats independents de reconeguda solvència. Tindran la consideració de normes europees o internacionals, ISO/IEC 15408, o altres de naturalesa i qualitat anàlogues. Tindran la consideració d'entitats independents de reconeguda solvència les recollides en els acords o disposicions internacionals de reconeixement mutu dels certificats de la seguretat. Atés que la llista dels productes certificats és molt extensa i podria quedar obsoleta per la certificació de nous productes, es recomana consultar les llistes actualitzades de productes certificats dels organismes d'acreditació i certificació anteriors.

Quan es reclamen algorismes o protocols acreditats pel CCN prevaldrà l'indicat en l'apartat N/SEG/TEC-014-2.

N/SEG/TEC-014-2 ALGORISMES I PROTOCOLS ACREDITATS

S'utilitzaran els algorismes i protocols criptogràfics que es consideren acreditats pel CCN per al seu ús dins de l'Esquema Nacional de Seguretat, quan les seues característiques i requeriments es consideren necessaris.

N/SEG/TEC-014-3 PROTECCIÓ DE CLAUS CRIPTOGRÀFIQUES

La protecció de les claus de xifratge, independentment de la seguretat que oferisquen, complirà els requisits següents:

• La protecció abastarà tot el cicle de vida de les claus: La seua generació, el transport al punt d'explotació, la custòdia durant l'explotació, l'arxivament posterior a la seua retirada d'explotació activa i la destrucció final.

• S'ha de garantir que les claus generades són imprevisibles.

• Els mitjans de generació han d'estar aïllats dels mitjans d'explotació. Les claus han de generar-se en un equip i després traslladar-se a l'equip en el qual s'usaran. Els elements de generació que no siguen necessaris per a l'ús es quedaran en l'equip de generació. És molt recomanable emprar un suport d'informació (per exemple, un disc USB o una targeta de memòria) per a traslladar les claus.

• En el transport o distribució al punt d'utilització s'ha d'assegurar la confidencialitat de la clau i l'autenticitat del receptor. Si s'opta pel lliurament en

mà, s'utilitzaran contenidors físics segurs. En un altre cas, s'usaran contenidors criptogràfics. Cap la distribució per doble canal, clau i dades d'activació per separat.

• S'utilitzaran mitjans de generació i custòdia en explotació avaluats o dispositius criptogràfics certificats. Aquests mitjans usaran algorismes acreditats pel CCN.

• Els mitjans de custòdia en explotació hauran d'emprar targeta intel·ligent protegida per contrasenya. S'ha de procurar el seu canvi quan el volum de dades xifrades o el temps que porta en ús superen els paràmetres recomanats abans que un atacant puga descobrir-la per anàlisi de les dades xifrades.

• Las claus retirades d'operació que hagen de ser arxivades, ho seran en mitjans aïllats dels d'explotació (p. ex., en contenidors físics segurs o en contenidors criptogràfics). El Comité de Seguretat TIC determinarà, quan una clau es retira d'explotació, durant quant de temps s'ha de retindre, bé per raons operatives, bé com a prova d'auditoria. És molt recomanable que les claus que es retenen estiguen en equips separats. Per al seu ús es traslladarà la informació a l'equip on estiguen.

• Quan s'hi haja de procedir a la destrucció de claus s'eliminarà l'original i totes les seues còpies. S'observarà el que es disposa en l'apartat N/SEG/TEC-016-2.

• Hi haurà un registre que indique les actuacions realitzades sobre cada clau en el sistema al llarg del seu cicle de vida.

N/SEG/TEC-015 NETEJA DE DOCUMENTS

S'haurà de procedir a la neteja de documents electrònics, de manera que s'hi retire tota la informació addicional continguda en camps ocults, metadades, comentaris o revisions anteriors, excepte quan aquesta informació siga pertinent per al receptor del document o resulte imprescindible per a la gestió correcta dels documents.

Aquesta mesura és especialment rellevant quan el document es difon àmpliament, com ocorre quan s'ofereix al públic en un servidor web o un altre tipus de repositori d'informació.

Es tindrà present que l'incompliment d'aquesta mesura pot perjudicar:

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

Haurà d'haver-hi un procediment per a netejar tots els documents que seran transferits a un altre domini de seguretat i per a netejar tots els documents que seran publicats electrònicament.

S'utilitzaran eines avaluades d'anàlisis de metadades i per a netejar les dades ocultes innecessàries dels documents, incloses les metadades existents en fitxers adjunts a correus electrònics.

N/SEG/TEC-016 SUPORTS ELECTRÒNICS

Els suports electrònics d'informació inclouen:

• Discos dels servidors i equips d'usuari final, amb especial consideració als equips mòbils (portàtils i telèfons intel·ligents) i discos removibles
• PDA
• Telèfons intel·ligents
• Disquets, cintes, CD, DVD...
• Discos USB
• Targetes de memòria i targetes intel·ligents
• Componentes d'impressores
• Altres mitjans electrònics d'emmagatzematge d'informació amb capacitat perquè la informació puga ser recuperada de forma automàtica o manual.

N/SEG/TEC-016-1 GESTIÓ DE SUPORTS

La gestió dels suports d'informació s'ajustarà al que es disposa en la norma N/SEG/USU-002-4. Sense perjudici de l'anterior, en el Servei d'Informàtica seran aplicables, a més, les directrius següents:

• Segons el tipus de suport, s'aplicaran mesures contra la seua degradació o destrucció, i es determinaran els períodes de validesa dels suports, atesa la caducitat dels materials utilitzats en la seua fabricació.

• Els suports que continguen informació necessària per a garantir la continuïtat dels sistemes en cas de contingència hauran d'emmagatzemar-se allunyats de l'equip del qual s'ha extret la informació, en dispositius que dificulten seriosament la seua exposició a agressions de tipus físic o químic. Caldrà conservar un duplicat d'aquests suports en un establiment o local diferent del que se situen els equips esmentats.

• Els suports que siguen remesos al Servei d'Informàtica per al seu esborrament segur i/o destrucció s'hauran d'anotar també en el registre d'entrades i, si escau, d'eixides de suports d'aquest Servei. Després de l'esborrament o destrucció, es lliurarà un document de constància del procediment dut a terme, el resultat i l'estat final del suport. Una còpia del document de constància es farà arribar al remitent del suport.

• Els suports que, per qualsevol tipus d'avaria o funcionament defectuós, requeriren del seu trasllat a locals de tercers hauran de fer-ho sense albergar-hi cap mena d'informació, i se'ls aplicarà prèviament un procediment d'esborrament segur, tal com es descriu en l'apartat N/SEG/TEC-016-2.

N/SEG/TEC-016-2 ESBORRAMENT SEGUR I DESTRUCCIÓ

Els suports que hagen de ser reutilitzats per a una altra informació, enviats a una altra organització o destruïts seran objecte d'un esborrament segur del seu contingut. El mètode d'eliminació de la informació dependrà del nivell de sensibilitat d'aquesta:

a) Informació classificada com a PÚBLICA. L'esborrament s'efectuarà mitjançant els comandos d'esborrament facilitats per la plataforma utilitzada o utilitats generals, o a través de la recuperació del format original del dispositiu.

b) Informació classificada com a RESERVADA, RESTRINGIDA, CONFIDENCIAL i dades de caràcter personal de categories especials. L'esborrament s'efectuarà mitjançant mètodes de sobreescriptura basada en dades, que garantisquen l'accés a totes les àrees del suport a esborrar i que proporcionen pistes d'auditoria d'allò esborrat. La sobreescriptura de tota la informació es portarà a terme en tres fases: La primera amb un

valor, la segona amb el complement a 1 d'aquest, i la tercera amb un valor aleatori. Després d'aquest procés s'ha de verificar que tota la informació s'ha reescrit i que no han aparegut errors maquinari en el procediment. Cas d'aparéixer errors s'acudirà a la desmagnetització.

Quan la naturalesa del suport no permeta l'esborrament segur o quan així ho requerisca el procediment associat a la informació continguda, es destruiran de manera segura els suports. La destrucció física de qualsevol suport electrònic d'informació haurà d'anar precedida d'un procés d'esborrament que garantisca la impossibilitat de recuperació de qualsevol tipus de dada, mitjançant la transformació del mitjà en inservible. S'utilitzaran per a això eines de maquinari del tipus desmagnetitzador o similar, que estiguen certificades conforme al que s'estableix en l'apartat N/SEG/TEC-021-3.

S'usaran productes o serveis que complisquen el que s'estableix en [op.pl.5] per al correcte esborrament segur i destrucció.

El procediment per a l'esborrament segur i destrucció de suports d'informació contindrà les instruccions precises per al compliment de la present norma atesos els diferents tipus de suport.

N/SEG/TEC-017 SEGURETAT D'INSTAL·LACIONS

Els llocs on es troben instal·lats els equips físics que donen suport als sistemes d'informació es classificaran en **Crítics (C)** i **No Crítics (NC)**.

Es qualificaran com a **Crítiques** aquelles instal·lacions que alberguen o continguen equips que resulten estratègics per la seua importància en el funcionament regular dels sistemes d'informació, la seguretat de la informació i l'impacte en els serveis públics.

N/SEG/TEC-017-1 CONDICIONES DE LAS INSTALACIONES

L'equipament s'instal·larà en àrees separades específiques per a la seua funció. A aquestes àrees separades només es podrà accedir per les entrades previstes i vigilades. Únicament tindran accés a l'àrea les persones degudament autoritzades. S'hi habilitaran dispositius que impedisquen l'accés no autoritzat. En instal·lacions No Crítiques (NC), com a mínim, les sales han d'estar tancades i disposar d'un control de claus.

Els locals on se situen els sistemes d'informació i els seus components han de comptar amb la potència elèctrica necessària. Es disposarà d'una anàlisi de la potència elèctrica requerida, que s'actualitzarà abans de l'adquisició de nous components. S'haurà de comptar amb les preses elèctriques necessàries. D'igual manera, es garantirà el funcionament correcte de les llums d'emergència, mitjançant la revisió periòdica d'aquestes. Serà obligatori, en el cas d'instal·lacions Crítiques (C), incorporar mecanismes que garantisquen el subministrament de potència elèctrica en cas de fallada del subministrament general (compost per SAI i, en cas de ser necessari, grup electrogen), de manera que es compte amb temps suficient per a una finalització ordenada dels processos, i salvaguardar la informació.

Els locals disposaran de les condicions adequades de temperatura i humitat, ateses les especificacions dels fabricants dels equips. S'hi instal·laran mecanismes que permeten el control dels valors recomanats.

Els locals comptaran amb les proteccions adequades contra les amenaces identificades en l'anàlisi de riscos, tant d'índole natural com derivades de l'entorn o amb origen humà, accidental o deliberat. El cablejat disposarà de la protecció adequada, mitjançant el seu etiquetatge (per a poder determinar les connexions de cada cable físic), protecció (per a evitar ensopegades) i control (per a evitar l'existència de cablejat fora d'ús). Es disposarà d'un pla del cablejat que incloga l'etiquetatge dels cables.

Es protegiran els locals contra els incendis, fortuïts o deliberats, conforme a la normativa industrial pertinent. De la mateixa manera, es protegiran els locals contra incidents fortuïts o deliberats causats per l'aigua, conforme al nivell de risc identificat, la qual cosa comporta la realització d'un estudi de la ubicació física del local per a conéixer el risc real de problemes per causa natural o per l'entorn.

N/SEG/TEC-017-2 ÚS DE LES INSTAL·LACIONS

Exclusivament el personal autoritzat podrà tindre accés als llocs on es troben instal·lats els equips físics que donen suport als sistemes d'informació. Hi haurà un llistat de les persones autoritzades.

El control d'accés a aquestes àrees s'efectuarà mitjançant mecanismes que permeten identificar inequívocament la persona que hi accedeix, com la data i l'hora d'entrada i eixida. Es portarà un registre en el qual conste tota la informació d'accés anterior. El registre serà automatitzat en cas d'instal·lacions Crítiques (C). Quan es tracte d'instal·lacions No Crítiques (NC) el registre podrà no estar automatitzat, i en aquest cas haurà de fer-se constar també la persona que

efectua el registre. Les dades del registre d'accessos es mantindran, com a mínim, durant un període de sis mesos.

Quan es realitzen visites autoritzades a aquestes instal·lacions, els visitants hauran de portar una identificació visible i estar acompanyats en tot moment per la persona designada per l'autoritzador.

Està prohibida l'existència de material innecessari en el local, en particular, material inflamable (paper, caixes, etc.) o que puga ser causa d'altres incidents (fonts d'aigua, plantes, etc.), i evitar que el local mateix puga ser una amenaça o atraga altres amenaces.

La permanència a les sales es limitarà al temps imprescindible per a complir la tasca que justifica l'accés. Està prohibit menjar, beure o practicar qualsevol activitat que puga generar una amenaça per a les instal·lacions o els equips que alberga. Quan siguen necessàries tasques de manteniment o reparació que comporten l'ús d'agents físics o químics agressius (foc, gas, eines, etc.) s'hauran d'extremar les precaucions i fer-se conforme a la normativa industrial i els bons usos professionals.

Haurà de mantindre's un registre detallat de tota entrada i eixida d'equipament. El registre ha de reflectir: Data i hora, identificació inequívoca de l'equipament, persona que realitza l'entrada o eixida, persona que autoritza l'entrada o eixida i persona que realitza el registre. Les dades del registre d'entrades i eixides d'equipament es mantindran, com a mínim, durant un període de dotze mesos. El registre el portarà el responsable de l'equipament, mentre siga responsable d'aquests actius del sistema.

N/SEG/TEC-017-3 INSTAL·LACIONS ALTERNATIVES

En cas que les instal·lacions habituals no es troben disponibles, quan alberguen equips de suport a sistemes de categoria ALTA o perquè ho aconselle l'anàlisi de riscos, haurà de garantir-se l'existència i disponibilitat d'instal·lacions alternatives. Aquestes instal·lacions alternatives hauran de comptar amb idèntiques garanties de seguretat que les instal·lacions habituals.

N/SEG/TEC-018 INCIDENTS DE SEGURETAT

N/SEG/TEC-018-1 CATEGORITZACIÓ D'INCIDENTS

Per a la seua correcta gestió, tots els incidents hauran d'estar classificats. La classificació d'incidents de seguretat dependrà de diversos factors, com:

- La naturalesa de l'incident
- La criticitat del sistema o sistemes afectats
- El nombre de sistemes afectats
- L'impacte que l'incident pot tindre en l'organització des d'un punt de vista legal, d'imatge pública, i de prestació de servei
- Els requeriments legals i reguladors

Un incident que continga múltiples classes o tipologies ha de ser classificat per l'esdeveniment de seguretat original o detectat inicialment.

Es conformarà la categorització d'incidents seguint les directrius de la guia CCN-STIC 817.

N/SEG/TEC-018-2 CRITERIS PER A LA DETERMINACIÓ DE LA CRITICITAT

Per a poder fer el seguiment correcte, determinar les prioritats i assignar recursos, és essencial que per a cada incident es determine quin nivell de criticitat se li assigna. S'emprarà una escala de criticitat amb **5 nivells:**

A) Nivell de criticitat **BAIX**. Es classifiquen amb aquest nivell de criticitat els casos d'incidents en què es té constància de l'existència d'una amenaça que ha afectat o està afectant sistemes TIC de l'organització, però que els controls de seguretat desplegats estan funcionant i la contraresten

adequadament i, per tant el seu impacte és nul o insignificant per a l'organització.

B) Nivell de criticitat **MITJÀ**. Es classifiquen amb aquest nivell de criticitat els casos d'incidents en què es té constància de l'existència d'una amenaça que ha afectat o està afectant sistemes TIC de l'organització, i se sap que ha tingut un impacte limitat en informació considerada no crítica per a la missió de l'organització i/o sistemes TIC no crítics en l'arquitectura dels sistemes TIC de l'organització.

C) Nivell de criticitat **ALT**. Es classifiquen amb aquest nivell de criticitat els casos d'incidents en què es té constància de l'existència d'una amenaça que ha afectat o està afectant sistemes TIC de l'organització, i se sap que ha tingut un impacte considerable (afectació a la confidencialitat, disponibilitat o integritat) en informació considerada no crítica per a la missió de l'organització i/o sistemes TIC no crítics en l'arquitectura dels sistemes TIC de l'organització.

D) Nivell de criticitat **MOLT ALT**. Es classifiquen amb aquest nivell de criticitat els casos d'incidents en què es té constància de l'existència d'una amenaça que ha afectat o està afectant sistemes TIC de l'organització, i se sap que ha tingut un impacte considerable (afectació a la confidencialitat, disponibilitat o integritat) en informació considerada crítica per a la missió de l'organització i/o sistemes TIC crítics en l'arquitectura dels sistemes TIC de l'organització .

E) Nivell de criticitat **CRÍTIC**. Es classifiquen amb aquest nivell de criticitat els casos d'incidents en què es té constància de l'existència d'una amenaça que ha afectat o està afectant sistemes TIC de l'organització, i se sap que ha tingut un impacte molt considerable (afectació total de la confidencialitat, disponibilitat o integritat) en informació considerada crítica

per a la missió de l'organització i/o sistemes TIC crítics en l'arquitectura dels sistemes TIC de l'organització.

N/SEG/TEC-018-3 GESTIÓ D'INCIDENTS

S'establirà un procediment que contemple la gestió integral dels incidents de seguretat: Comunicació, registre, tractament, resposta i comunicació, si s'escau, al CSIRT d'àmbit autonòmic.

Quan es produïsquen "alertes de seguretat" que hagen de ser comunicades als usuaris dels sistemes d'informació, aquestes es canalitzaran a través del responsable de Seguretat dels Sistemes d'Informació.

N/SEG/TEC-018-4 GRUP DE RESPOSTA A INCIDENTS TIC

En compliment de l'article 15 del Reglament pel qual es regula la política de seguretat i de la protecció de dades de caràcter personal en la Diputació Provincial de València s'haurà de crear un Grupo de Resposta a Incidents TIC (Grup RITIC), la funció del qual serà la presa urgent de decisions en cas de contingència greu que afecte la seguretat de sistemes d'informació crítics de la corporació. El Grup RITIC estarà format per membres designats pel Comité de Seguretat TIC.

Caldrà d'elaborar un procediment que establisca la forma d'actuació del Grup RITIC en cas de desastre.

N/SEG/TEC-019 ASSISTÈNCIA REMOTA

Quan s'utilitzen eines d'assistència tècnica remota que impliquen el control remot de l'ordinador o dispositiu de l'usuari, haurà de recaptar-se prèviament el consentiment informat de l'usuari. S'intentarà habilitar mecanismes automatitzats que proporcionen la condició anterior i la constància d'això. Les eines d'assistència remota hauran de comptar amb registres d'activitat que deixen evidència de les accions executades.

N/SEG/TEC-020 GARANTIA DE CONTINUÏTAT DELS SISTEMES

N/SEG/TEC-020-1 CÒPIES DE SEGURETAT

Correspon al Servei d'Informàtica la realització de còpies de seguretat i recuperació de la informació de tots els sistemes d'informació, com també del programari que els tracta, de manera que queden a resguard de qualsevol contingència que en puga comportar la pèrdua o comprometre la integritat.

Tal com s'estableix en la norma N/SEG/USU-001-6, en els casos en què s'autoritze la ubicació de la informació en l'estació de treball de l'usuari mateixa o en servidors o equips no corporatius, l'usuari serà responsable de la integritat i còpia de seguretat de la informació i, per tant, de la seua pèrdua o modificació.

Les còpies de seguretat hauran d'abastar, com a mínim:

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 a preservar la confidencialitat de la informació.

La periodicitat de la còpia de seguretat de cada informació es fixarà tenint en compte els riscos i com de crítica siga la informació, i no podrà ser major a set dies el temps transcorregut des que una dada és introduïda en el sistema fins que és salvada.

S'haurà de mantindre un registre, si no el produeix automàticament el programari mateix emprat en la realització de les *còpies de seguretat*, que permeta conéixer per a cada informació la data en què es va realitzar l'última còpia, la identificació del suport físic en el qual es va fer i la ubicació d'emmagatzematge d'aquest.

S'haurà d'elaborar un procediment en el qual es continguen els plans de realització de còpies de seguretat i recuperació dels sistemes d'informació corporatius. Aquests plans recolliran els mètodes, la periodicitat i les eines, així com l'antiguitat de conservació de les còpies. El procediment inclourà les actuacions, el personal responsable i les autoritzacions, si s'escau, que corresponguen.

Qualsevol modificació en el sistema que afecte dades de caràcter personal, com pot ser la implantació de noves aplicacions, creació de nous fitxers, etc., haurà de ser contemplat immediatament en el pla de recuperació, de manera que aquesta nova informació quede fora de perill.

Les còpies de seguretat posseiran el mateix nivell de seguretat que les dades originals pel que fa a integritat, confidencialitat, autenticitat i traçabilitat. En particular, es considerarà la conveniència o necessitat, segons siga procedent, que les còpies de seguretat estiguen xifrades per a garantir la confidencialitat.

Per a garantir la validesa dels procediments de salvaguarda s'hauran de realitzar comprovacions de la integritat i consistència de la informació que contenen, i que les reserves són capaces de recuperar la informació perduda davant l'ocurrència

d'un esdeveniment hipotètic. Quan es tracte de dades de caràcter personal, caldrà verificar semestralment la fiabilitat de les còpies de seguretat.

Per a la recuperació d'informació de les còpies de seguretat serà necessària l'autorització corresponent, en els termes recollits en l'apartat N/SEG/TEC-003.

La recuperació de dades es considerarà un incident de seguretat, i s'haurà d'anotar en el registre indicat en la norma N/SEG/USU-006-2. El procediment de gestió d'incidents, al qual es refereix l'apartat N/SEG/TEC-018-3, establirà la informació que haja d'anotar-se en aquest registre.

Únicament en el cas que la pèrdua o destrucció afectara fitxers o tractaments de dades de caràcter personal parcialment automatitzats, i sempre que l'existència de documentació permeta aconseguir l'objectiu de reconstrucció en l'estat en què es trobaven en el moment de produir-se la pèrdua o destrucció, s'haurà de procedir a gravar manualment les dades i quedarà constància motivada d'aquest fet en el document de seguretat.

Els suports de còpies de seguretat s'ajustaran al que s'estableix en l'apartat N/SEG/TEC-016-1. Quan es tracte de dades de caràcter personal de nivell ALT, a més:

• S'haurà de conservar una còpia de seguretat i dels procediments de recuperació de les dades en un lloc diferent d'aquell en què es troben els equips informàtics.

• A les còpies de dades emmagatzemades fora del lloc de treball se'ls ha de donar el mateix nivell de seguretat que a les que residisquen en les dependències de l'organització.

• S'haurà mantindre un inventari del contingut que es troba en els llocs d'emmagatzematge externs.

N/SEG/TEC-020-2 ANÀLISI D'IMPACTE

Aquells sistemes la dimensió de disponibilitat dels quals siga de nivell MITJÀ o ALT hauran de sotmetre's a una anàlisi d'impacte, és a dir, a un estudi detallat de com afectaria un desastre a la prestació de serveis, i identificar els elements del sistema d'informació que són necessaris per a la prestació de cada servei.

Haurà d'elaborar-se un procediment amb els criteris i passos a seguir per a la realització de l'anàlisi d'impacte.

N/SEG/TEC-020-3 PLA DE CONTINUÏTAT

Haurà de desenvolupar-se un Pla de Continuïtat que establisca les accions a executar en cas d'interrupció dels serveis prestats amb els mitjans habituals. Aquest Pla haurà de contemplar obligatòriament tots els sistemes crítics i aquells la dimensió de disponibilitat dels quals siga de nivell ALT. El Pla serà aprovat pel Comité de Seguretat TIC.

Aquest Pla contemplarà els aspectes següents:

a) Caldrà identificar funcions, responsabilitats i activitats a realitzar en cas de desastre que impedisca prestar el servei en les condicions habituals i amb els mitjans habituals. En particular:

   - Els qui componen el comité de crisi que pren la decisió d'aplicar els plans de continuïtat després d'analitzar el desastre i avaluar les conseqüències.

- Els qui s'encarregaran de la comunicació amb les parts afectades en cas de crisi.
- Els qui s'encarreguen de reconstruir el sistema d'informació (recuperació de desastre).

b) Ha d'haver-hi una previsió dels mitjans alternatius que s'han de conjugar per a poder continuar prestant els serveis en cas que no s'hi puga fer amb els mitjans habituals:

- Instal·lacions alternatives.
- Comunicacions alternatives.
- Equipament alternatiu.
- Personal alternatiu.
- Recuperació de la informació amb una antiguitat no superior a un límit determinat a la llum de l'anàlisi d'impacte.

c) El servei alternatiu oferirà les mateixes garanties de seguretat que el servei habitual. El pla ha de determinar la coordinació de tots els elements per a aconseguir la restauració dels serveis en els terminis estipulats. Tots els mitjans alternatius han d'estar planificats, i materialitzats en acords o contractes amb els proveïdors corresponents, si s'escau.

d) Les persones afectades pel pla han de rebre formació específica relativa al seu paper en aquest pla.

e) El pla de continuïtat ha de ser part integral i harmònica amb els plans de continuïtat de l'organització en altres matèries alienes a la seguretat.

f) Han d'establir-se procediments per a sincronitzar el pla de continuïtat amb les actualitzacions del sistema referent a arquitectura, elements components i serveis i qualitat dels serveis prestats; és a dir, els

procediments operatius de seguretat referents a canvis i actualitzacions han d'incloure un punt per a actualitzar els plans de continuïtat.

Es realitzaran proves periòdiques per a localitzar i corregir, si s'escau, els errors o les deficiències que puguen existir en el pla d'acció en cas de desastre.

Després de cada exercici ha de fer-se un informe d'anàlisi de les proves realitzades, s'hi destacaran les incidències pròpies o en els proveïdors externs i es derivarà un pla de millores, tant en els mitjans com en els procediments i en la conscienciació i formació de les persones implicades.

N/SEG/TEC-021 CONTRACTACIÓ

N/SEG/TEC-021-1 ADQUISICIÓ DE MAQUINARI I PROGRAMARI

Per a efectuar la selecció d'equips i paquets de programari s'avaluaran, entre d'altres, els aspectes següents:

• Facilitat i amigabilitat d'ús.

• Manteniment senzill del producte, que no implique costos addicionals.

• Compatibilitat i independència d'un maquinari o programari específic.

• Cicle de vida de la instal·lació o programari, amb desenvolupament de noves versions de millora o adaptació a canvis tecnològics.

• Evitar, sempre que siga possible, un programari amb protecció de còpies, que dificulte la recuperació del sistema en moments d'emergència.

• El volum de descompte per compres múltiples, i les condicions de la llicència.

• La cobertura d'assistència tècnica.

• Seguretat física i lògica.

El Servei d'Informàtica efectuarà la selecció d'equipament i paquets de programari. Per això, elaborarà una anàlisi tècnica de costos comparatius, enfocada a les necessitats de l'usuari final, i valorarà entre altres factors el preu del producte i els condicionants (formació, instal·lació, manteniment, entrada de dades, etc.) que implica la seua posada en funcionament.

Es consideraran especialment com a factors favorables per a l'adquisició d'un producte o equip l'existència en els contractes de compra o lloguer de clàusules

de manteniment, actualització de versions, servei de suport tècnic i formació en el producte.

Haurà d'establir-se un procés formal per a planificar l'adquisició de nous components del sistema, que contemple el que es preveu en aquesta norma i que a més:

- Tinga en compte l'anàlisi de riscos.
- S'ajuste a l'arquitectura de seguretat triada.
- Preveja els recursos necessaris, l'esforç i els mitjans econòmics per a la implantació inicial, el manteniment al llarg de la seua vida útil i l'evolució de la tecnologia.
- Atenga en tot moment tant les necessitats tècniques com la conscienciació necessària i la formació de les persones que treballaran amb els components.

Tot això sense perjudici del que s'estableix en l'apartat N/SEG/TEC-007-2, en aquells supòsits que resulte d'aplicació.

N/SEG/TEC-021-2 CONTRACTACIÓ DE SERVEIS

Quan s'utilitzen recursos externs a la corporació, siguen serveis, equips, instal·lacions o personal, s'haurà de tindre en compte que la delegació es limita a les funcions. La corporació continua sent en tot moment responsable dels riscos en què s'incorre, en la mesura en què impacten sobre la informació manejada i els serveis finals prestats. Per això es cal disposar les mesures necessàries perquè la Diputació puga exercir la seua responsabilitat i mantindre el control en tot moment, tal com estableix l'apartat N/SEG/TEC-001-3.

Amb caràcter general, quan s'haja de procedir a la contractació de serveis externs es tindrà en compte que:

• Han de contractar-se serveis que compten amb la certificació d'ENS conforme a la categoria del sistema on s'implantarà.

• Han d'establir-se contractualment les característiques del servei prestat i les responsabilitats de les parts. Es detallarà el que es considera qualitat mínima del servei prestat i les conseqüències del seu incompliment (acords de nivell de servei).

• Resulta aconsellable realitzar prèviament una anàlisi de riscos que identifique els riscos associats al proveïdor extern.

• Si implica tractament de dades de caràcter personal, s'ha de garantir l'aplicació de la normativa interna en la matèria (N/PDP); ha de considerar-se especialment:

- L'existència d'encarregat de tractament.
- Lloc de prestació dels serveis (locals de la Diputació o del proveïdor).
- Exigència de geolocalització.
- Cessions de dades.
- Subcontractació.

• Les garanties de seguretat de la informació, que quedaran detallades en el document contractual que resulte vinculant.

• És recomanable recollir de forma agrupada les condicions sobre confidencialitat, seguretat de la informació i protecció de dades de caràcter personal; com també utilitzar formats de condicions normalitzats.

Quan els serveis afecten sistemes de categoria MITJANA i superior:

• Haurà de realitzar-se una anàlisi de riscos que identifique els riscos associats al proveïdor extern.

• Haurà d'establir-se un contracte formal, aprovat per les dues parts i actualitzat periòdicament, establint:

- Rols i funcions de les dues parts en matèria de seguretat, inclosos els mecanismes de contacte.
- Obligacions i responsabilitats de cada part.
- Protocol d'avís previ d'actuacions que puguen impactar a l'altra part.
- Mecanismes i procediments per a la sincronització de les activitats de gestió d'incidències.

• Haurà d'establir-se un sistema rutinari per a mesurar el compliment de les obligacions de servei i el procediment per a neutralitzar qualsevol desviació fora del marge de tolerància acordat.

• Haurà d'establir-se el mecanisme i els procediments de coordinació per a dur a terme les tasques de manteniment dels sistemes afectats per l'acord, com també el mecanisme i els procediments de coordinació en cas d'incidents i desastres.

N/SEG/TEC-021-3 ADQUISICIÓ DE PRODUCTES I SERVEIS DE SEGURETAT

En l'adquisició de productes i serveis de seguretat de les TIC s'utilitzaran, de forma proporcionada a la categoria del sistema i el nivell de seguretat

determinats, aquells que tinguen certificada la funcionalitat de seguretat relacionada amb l'objecte de la seua adquisició, excepte en aquells casos en què les exigències de proporcionalitat quant als riscos assumits no ho justifiquen segons el parer del responsable de Seguretat dels Sistemes d'Informació.

La certificació indicada en l'apartat anterior haurà d'estar d'acord amb les normes i els estàndards reconeguts internacionalment en l'àmbit de la seguretat funcional. Tindran la consideració de normes europees o internacionals ISO/IEC 15408 o altres de naturalesa i qualitat anàlogues.

En el cas de sistemes de categoria ALTA s'utilitzaran sistemes, productes o equips les funcionalitats de seguretat dels quals i el seu nivell hagen sigut avaluats conforme a normes europees o internacionals i els certificats de les quals estiguen reconeguts per l'Esquema Nacional d'Avaluació i Certificació de la Seguretat de les Tecnologies de la Informació.

L'adquisició de les eines de seguretat descrites en l'apartat N/SEG/TEC-007-5 s'ajustarà a les pautes següents:

• Els requisits obligatoris de maquinari i programari de les eines de seguretat corresponents hauran d'especificar-se de manera detallada en els plecs de prescripcions tècniques, els contractes per a la seua adquisició o la proposta vinculant.

• Els recursos addicionals que es consideren necessaris per a l'adequada explotació de les eines de seguretat han d'estar reflectits i tinguts en compte.

• En tot cas, s'utilitzaran preferentment productes certificats quan implementen les funcionalitats i els mecanismes de seguretat següents:

- Mecanisme d'autenticació

- Protecció de claus criptogràfiques
- Protecció de la confidencialitat
- Protecció de l'autenticitat i de la integritat
- Criptografia
- Esborrament i destrucció
- Firma electrònica
- Segells de temps

Les eines de xifratge programari constitueixen un grup especial, que es regirà pel que es disposa en l'apartat N/SEG/TEC-014.

La seguretat dels sistemes estarà atesa, revisada i auditada per personal qualificat, en els termes recollits en l'apartat N/SEG/TEC-024 lletra f).

Haurà d'exigir-se, de manera objectiva i no discriminatòria, que les organitzacions que presten serveis de seguretat dels sistemes a la corporació compten amb uns nivells idonis de gestió i maduresa en els serveis prestats i amb professionals qualificats.

Totes les eines i serveis de seguretat que s'utilitzen hauran de ser prèviament aprovats pel responsable de Seguretat dels Sistemes d'Informació.

N/SEG/TEC-022 ANÀLISI I GESTIÓ DE RISCOS

N/SEG/TEC-022-1 ASPECTES BÀSICS

L'anàlisi i gestió de riscos serà part essencial del procés de seguretat i haurà de mantindre's permanentment actualitzada. L'anàlisi de riscos ha de permetre:

- Validar el conjunt de mesures de seguretat implantat
- Detectar la necessitat de mesures addicionals
- Justificar l'ús de mesures de protecció alternatives

Tota anàlisi de riscos ha d'identificar i prioritzar els riscos més significatius a fi de conéixer els riscos als quals estan sotmesos els sistemes i prendre les mesures oportunes, tècniques o d'un altre tipus. Les mesures adoptades per a mitigar o suprimir els riscos hauran d'estar justificades i, en tot cas, hi haurà una proporcionalitat entre elles i els riscos.

Sense perjudici d'altres referències d'aquesta o altres normatives internes, que reclamen la necessitat de realitzar una anàlisi de riscos, haurà de realitzar-se una anàlisi de riscos:

a) Durant l'especificació d'un nou sistema, per a determinar els requisits de seguretat que han d'incorporar-se a la solució.
b) Durant el desenvolupament d'un nou sistema, per a analitzar opcions.
c) Durant l'operació del sistema, per a ajustar nous actius, noves amenaces, noves vulnerabilitats i noves salvaguardes.

El risc residual ha d'estar documentat i aprovat pel responsable de la informació i del servei corresponent(s). El Comité de Seguretat TIC determinarà a cada moment el nivell de risc assumible per l'organització per als seus sistemes d'informació.

Haurà d'elaborar-se un procediment per a l'anàlisi i la gestió de riscos. El procediment inclourà els criteris utilitzats per a seleccionar i valorar actius, amenaces i salvaguardes. Tot procés d'anàlisi de riscos quedarà documentat.

N/SEG/TEC-022-2 CRITERIS I METODOLOGIA

La realització de l'anàlisi de riscos estarà en funció de la categorització de cada sistema:

a) Sistemes de categoria BÀSICA o sense categoritzar. L'anàlisi de riscos pot ser informal, és a dir, duta a terme en un llenguatge natural en el qual serà suficient identificar els aspectes següents:

   - Els actius més valuosos del sistema
   - Les amenaces més probables
   - Les salvaguardes que protegeixen d'aquestes amenaces
   - Els principals riscos residuals

b) Sistemes de categoria MITJANA. S'haurà de realitzar una anàlisi semi-formal, usant un llenguatge específic, amb un catàleg bàsic d'amenaces i una semàntica definida. És a dir, una presentació amb taules que descriga els aspectes següents:

   - Identificació i valoració qualitativa dels actius més valuosos del sistema
   - Identificació i quantificació de les amenaces més probables
   - Identificació i valoració de les salvaguardes que protegeixen d'aquestes amenaces
   - Identificació i valoració del risc residual

c) Sistemes crítics i de categoria ALTA. S'haurà de realitzar una anàlisi formal, usant un llenguatge específic, amb un fonament matemàtic reconegut internacionalment. L'anàlisi haurà de cobrir els aspectes següents:

- Identificació i valoració qualitativa dels actius més valuosos del sistema
- Identificació i quantificació de les amenaces més probables
- Identificació de les vulnerabilitats habilitants d'aquestes amenaces
- Identificació i valoració de les salvaguardes adequades
- Identificació i valoració del risc residual

Per als supòsits b) i c) s'utilitzarà preferentment MAGERIT, la metodologia d'anàlisi i gestió de riscos elaborada pel Consell Superior d'Administració Electrònica (Ministeri d'Hisenda i Administracions Públiques), i serà convenient emprar alguna eina de suport, tant per a l'execució material com per a afrontar l'actualització regular dels càlculs davant noves amenaces o canvis en el sistema.

Tot això conciliat amb el que s'estableix en l'apartat N/SEG/TEC-001-1.

N/SEG/TEC-023 AUDITORIA DE LA SEGURETAT

N/SEG/TEC-023-1 OBJECTE I TIPUS D'AUDITORIA

En funció del seu objecte, es distingiran dos tipus d'auditoria de seguretat:

a) Auditories compreses en el Pla General Auditor de Protecció de Dades Personals i Seguretat de la Informació de la Diputació, que tindran caràcter periòdic per a avaluar el compliment de la normativa sobre seguretat i l'efectivitat de les mesures adoptades. Són les dutes a terme pel Departament de Protecció de Dades i Seguretat de la Informació, en compliment de l'article 35 del Reglament pel qual es regula la política de seguretat i de la protecció de dades de caràcter personal de la Diputació de València.

   A més, el delegat de Protecció de Dades haurà de supervisar aquestes auditories, en virtut del que s'estableix en l'article 37 del reglament citat.

b) Auditories, regulars o extraordinàries, en compliment del RGPD i de l'Esquema Nacional de Seguretat. L'objecte d'aquestes auditories de la seguretat, internes o externes, és l'establit en les normes N/SEG/USU-004-3 i N/SEG/USU-008. Són auditories obligatòries i de caràcter reglamentari.

N/SEG/TEC-023-2 AUDITORIES DEL DEPARTAMENT DE PROTECCIÓ DE DADES I SEGURETAT DE LA INFORMACIÓ

Les auditories dutes a terme pel Departament de Protecció de Dades i Seguretat de la Informació, i, si s'escau, supervisades pel delegat de Protecció de Dades,

estaran determinades en un procediment documentat que recollirà, com a mínim, les qüestions següents:

- Objectius de control
- Metodologia
- Instruments o eines
- Periodicitat
- Informes

Els informes de resultats de les auditories periòdiques que afecten tractaments de dades de caràcter personal es gestionaran d'acord amb les indicacions del Departament de Protecció de Dades i Seguretat de la Informació i a la disposició de l'Agència Espanyola de Protecció de Dades o, si escau, de les autoritats de control de la Comunitat Autònoma.

N/SEG/TEC-023-3 AUDITORIES REGLAMENTÀRIES

Les auditories reglamentàries comprenen:

a) La verificació ordinària (biennal) o extraordinària (puntual) del compliment dels requeriments de seguretat establits per la normativa legal d'aplicació i, en particular, pel Reglament pel qual es regula la política de seguretat i de la protecció de dades de caràcter personal de la Diputació de València i la seua normativa de desenvolupament.

b) La verificació ordinària (biennal) o extraordinària (puntual) del compliment de les mesures de seguretat aplicables als sistemes d'informació i instal·lacions de tractament i emmagatzematge de dades de caràcter personal.

Les auditories reglamentàries s'ajustaran als requisits següents:

• Per motius d'eficiència i economia, aquestes auditories s'unificaran sempre que siga possible.

• Excepte en el supòsit a) de l'apartat N/SEG/TEC-023-4, l'equip auditor estarà compost per professionals de l'auditoria de seguretat de sistemes d'informació, així com per professionals, si s'escau, de l'auditoria en protecció de dades de caràcter personal, tots ells amb experiència contrastada i acreditacions reconegudes (ISACA, ISC, APEP…).

• En la realització de les auditories s'utilitzaran els criteris, mètodes de treball i de conducta generalment reconeguts, així com la normalització nacional i internacional aplicables a aquesta mena d'auditories de sistemes d'informació.

• L'auditoria es basarà en l'existència d'evidències que permeten sustentar objectivament el compliment dels punts sotmesos a control.

• L'informe d'auditoria haurà de dictaminar sobre l'adequació de les mesures i controls a la normativa legal, la reglamentaria i la interna de la corporació, identificar les seues deficiències i proposar les mesures correctores o complementàries necessàries, com també les recomanacions que es consideren oportunes. Igualment, haurà d'incloure els criteris metodològics d'auditoria utilitzats, l'abast i l'objectiu de l'auditoria, les dades, els fets i les observacions en què es basen els dictàmens aconseguits i les recomanacions proposades.

• Els informes d'auditoria seran analitzats pel responsable de Seguretat dels Sistemes d'Informació, que presentarà les seues conclusions al Comité de Seguretat TIC perquè adopte les mesures correctores adequades.

• Els informes de resultats de les auditories reglamentàries que afecten tractaments de dades de caràcter personal es gestionaran d'acord amb les indicacions del Departament de Protecció de Dades i Seguretat de la Informació i quedaran a la disposició de l'Agència Espanyola de Protecció de Dades o, si s'escau, de les autoritats de control de la Comunitat Autònoma.

• Haurà d'elaborar-se un procediment que reculla els requisits i les pautes de treball per a la realització de les auditories reglamentàries.

N/SEG/TEC-024 GESTIÓ DE LA SEGURETAT

L'Esquema Nacional de Seguretat exigeix l'existència un sistema de gestió de la seguretat de la informació, documentat i amb un procés regular d'aprovació per la direcció. El terme gestió de la seguretat descriu els processos i les activitats essencials necessàries per a l'establiment i el manteniment del programa de seguretat de tota organització.

En l'àmbit de la Diputació de València la gestió de la seguretat de la informació es regeix per:

a) Principi d'integritat. Tal com estableix l'article 11 del Reglament pel qual es regula la política de seguretat i de la protecció de dades de caràcter personal de la Diputació de València, la seguretat s'entendrà com un procés integral constituït per tots els elements tècnics, humans, materials i organitzatius, relacionats amb el sistema, per la qual cosa qualsevol acció dirigida a l'objectiu de la seguretat ha de considerar la interacció de tots els elements citats, exclòs qualsevol actuació puntual o tractament conjuntural.

b) Anàlisi i gestió de riscos. En aplicació de l'article 12 del reglament citat, la gestió de la seguretat es recolzarà en un procés continu d'anàlisi i tractament de riscos. Aquest procés haurà de mantindre's actualitzat de manera permanent. A tal objecte, se seguiran les indicacions de l'apartat N/SEG/TEC-022.

c) Monitoratge de la seguretat. És un procés continu que observa els sistemes i identifica els intents de comprometre la seguretat de l'organització. Per a això s'atendrà especialment el que s'estableix en l'apartat N/SEG/TEC-005-2.

d) Reavaluació periòdica. Les mesures de seguretat es reavaluaran i actualitzaran periòdicament, per a adequar la seua eficàcia a l'evolució constant dels riscos i sistemes de protecció, i arribarà fins i tot a un replantejament de la seguretat, si fora necessari. L'aplicació del que es disposa en l'apartat N/SEG/TEC-023 té aquesta reavaluació com a objectiu principal.

e) Millora contínua. El procés integral de seguretat implantat haurà de ser actualitzat i millorat de manera contínua. Tota estructura organitzativa necessita una avaluació constant i una anàlisi de la resposta als incidents de manera que s'aprén de l'experiència, es corregeixen defectes o febleses i es busca l'excel·lència per mitjà de la millora contínua. Per a això, s'aplicaran els criteris i mètodes reconeguts en la pràctica nacional i internacional relatius a gestió de les tecnologies de la informació. Haurà d'avaluar-se el cicle de maduresa del sistema de gestió de la seguretat, criteris per a la revisió i agenda de millores. S'aplicarà a tal fi el que es disposa en l'apartat N/SEG/TEC-005-3.

f) Professionalitat. La seguretat dels sistemes estarà atesa, revisada i auditada per personal qualificat, dedicat i instruït en totes les fases del seu cicle de vida: Instal·lació, manteniment, gestió d'incidents i

desmantellament. Tant si es tracta de personal intern com d'extern, la gestió de la seguretat correspondrà a professionals amb formació i experiència contrastable sobre les matèries concretes a tractar, que reunisquen les condicions, a més de les de coneixements i competència, d'actuar de manera independent. La independència, en el cas de personal de seguretat intern, s'ajustarà al que es preveu en l'article 16 de l'Esquema Nacional de Seguretat.

Tota la documentació generada per l'aplicació dels elements citats anteriorment forma part del sistema de gestió de la seguretat de la informació. Amb caràcter anual, el responsable de Seguretat dels Sistemes d'Informació prepararà un informe que reculla una síntesi d'aquesta documentació i les conclusions més rellevants, el qual traslladarà al Comité de Seguretat TIC perquè determine les possibles actuacions que considere oportunes, a la vista d'aquestes conclusions.

N/SEG/TEC-025 MARC DE RESPONSABILITATS

La responsabilitat del responsable de Seguretat dels Sistemes d'Informació, a la qual es refereix l'article 29 del Reglament pel qual es regula la política de seguretat i de la protecció de dades de caràcter personal de la Diputació de València, està limitada a l'execució de les comeses de determinar les mesures de seguretat que s'han d'implantar i de supervisar la seua correcta implantació.

La responsabilitat del responsable dels Sistemes d'Informació TIC i, si s'escau, dels responsables del sistema delegats, consisteix a cerciorar-se que les mesures específiques de seguretat determinades pel responsable de Seguretat s'integren adequadament en cada Sistema d'Informació TIC dins del marc general de seguretat.

La responsabilitat de l'administrador de Seguretat dels Sistemes d'Informació TIC i, si s'escau, dels administradors de Seguretat delegats, se circumscriu a la implantació, gestió i manteniment de les mesures de seguretat determinades pel responsable de Seguretat aplicables a cada Sistema d'Informació TIC.

La responsabilitat del Departament de Protecció de Dades i Seguretat de la Informació comprén la supervisió del compliment dels requisits legals i de la normativa interna en matèria de seguretat de la informació, en el marc de l'article 35 del Reglament pel qual es regula la política de seguretat i de la protecció de dades de caràcter personal de la Diputació de València.

Quan, en l'execució de la seua labor de supervisió, el responsable de Seguretat dels Sistemes d'Informació constate l'incompliment o inobservança de qualsevol mesura de seguretat haurà de comunicar-ho a qui considere responsable de la seua esmena. Aquests fets es consideraran incidents de seguretat i seran tractats conforme al que es disposa en l'apartat N/SEG/TEC-018-3.

N/SEG/TEC-026 INCOMPLIMENTS

Al personal al servei de la Diputació de València que incomplisca el que es preveu en la present normativa li serà aplicable el règim disciplinari establit per la legislació vigent per al personal al servei de l'Administració Pública que resulte

d'aplicació, sense perjudici que els fets puguen ser constitutius de responsabilitats en un altre ordre.

Quan els incompliments siguen comesos per tercers, sobre els quals recaiga l'obligació de compliment en virtut de contracte o qualsevol altre tipus de relació acordada, la responsabilitat els serà exigida en els termes previstos en els instruments que regulen aquestes relacions i per la normativa legal que puga resultar d'aplicació.