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 ALS USUARIS DELS SISTEMES D'INFORMACIÓ

CODI	N/SEG/USU	**APROVACIÓ**	Decret nº 15873, de 27 de desembre de 2022, del President de la Diputació

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
27/12/2022	01	01	Aprovació inicial de la norma

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

DATA D'EMISSIÓ: Desembre 2022

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 política citada 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 a integrada en el seu mandat la denominada Normativa de Seguretat, i en 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 núm. 15873, de 27 de desembre de 2022, el president de la Diputació de València ha aprovat les presents Normes de Seguretat per als Usuaris dels Sistemes d'Informació.

En el present document consta la normativa interna relacionada amb la seguretat dels sistemes d'informació de la Diputació de València que han de complir els usuaris d'aquests sistemes d'informació. D'acord amb l'article 4 del reglament citat, pel qual es regula la política de seguretat i de la protecció de dades de caràcter personal en la Diputació Provincial de València, la present normativa és aplicable a tots els departaments i les unitats de la Diputació de València, i resultarà d'obligat compliment per a tots els usuaris dels sistemes d'informació.

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 el BOP núm. 127 de 5 de juliol de 2022, i el recollit en el glossari següent:

«a) **Còpia de seguretat o de suport (*backup*)**: Còpia de la informació en un suport electrònic que possibilite la seua recuperació.

b) **Comité de Seguretat TIC**. És l'òrgan que gestiona i coordina la seguretat dels sistemes d'informació TIC de l'organització. El Comité es crea i regula en l'article 32 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 integrat pels membres següents:

- **President**. El cap de Servei d'Informàtica.
- **Vicepresident**. El secretari general de la corporació.
- **Secretari.** El responsable de Seguretat dels Sistemes d'Informació.
- **Vocals.** Els diferents responsables de sistemes d'informació delegats, responsables de seguretat delegats i administradors de seguretat delegats.
- **Una persona designada pel Departament de Protecció de Dades i Seguretat de la Informació,** que actuarà amb veu, però sense vot.
- **El delegat de Protecció de Dades de la Corporació,** que actuarà en funcions d'informació i assessorament en

matèria de protecció de dades, però no participarà en la presa de decisions.

c) **Fitxers temporals:** Fitxers de treball creats per usuaris o processos que són necessaris per a un tractament ocasional o com a pas intermedi durant la realització d'un tractament.

d) **Incident o incidència de seguretat:** Succés inesperat o no desitjat amb conseqüències en detriment de la seguretat del sistema d'informació en qualsevol de les seues cinc dimensions.

e) **Informació**: Tot tipus de dada en qualsevol format (digital o no automatitzat), que siga tractat per la Diputació de València en l'exercici de les seues competències.

f) **Responsable de la informació**: És qui té la potestat d'establir les característiques d'una informació a l'efecte de determinar els requisits en matèria de seguretat i de protecció de dades personals. Seran responsables de la Informació el personal directiu —caps de servei, caps d'oficina, directors/es, coordinadors/es, etc.— sota la direcció del qual es trobe la informació corresponent (articles 27 i 28 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.)

g) **Responsable de Seguretat dels Sistemes d'Informació**: És qui determina les decisions per a satisfer els requisits de seguretat de la informació i dels serveis, supervisarà la implantació de les mesures necessàries per a garantir que se satisfan els requisits i reportarà sobre totes aquestes qüestions. Serà responsable de Seguretat dels Sistemes

d'Informació en l'àmbit de la Diputació de València qui designe el Comité de Seguretat TIC (article 29 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.)

h) **Responsable del servei**: És qui té la potestat d'establir les característiques d'un servei, a l'efecte de determinar els requisits en matèria de seguretat i de protecció de dades personals. Seran responsables del servei el personal directiu —caps de servei, directors/es, etc.— sota la direcció del qual es trobe el servei corresponent (arts. 26 i 28 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).»

2. NORMATIVA INTERNA DE SEGURETAT PER ALS USUARIS DELS SISTEMES D'INFORMACIÓ

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

Queda exclosa de manera específica de l'aplicació de la present política la informació tractada pels grups polítics i/o els seus membres, les centrals sindicals i/o membres representants dels treballadors, sempre que aquesta informació no forme part dels actius d'informació titularitat de la corporació.

Quan la informació consistisca en dades de caràcter personal, a més de les presents disposicions s'aplicaran les específiques per a aquesta mena d'informació, contingudes en la Normativa de Protecció de Dades de Caràcter Personal, aprovada pel Decret núm. 15874, de 27 de desembre de 2022, del president de la Diputació.

N/SEG/USU-001 SEGURETAT DE LA INFORMACIÓ

Les normes de seguretat de la informació establides en la present normativa tenen caràcter de mínims. La seguretat podrà veure's incrementada en aquells supòsits en què així ho reclame la criticitat d'un sistema d'informació, per aplicació del principi de "seguretat coordinada i estructurada", establit 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, o per decidir-ho així l'organització a través del Comité de Seguretat TIC, mitjançant l'establiment de línies estratègiques de la seguretat dels sistemes d'informació.

N/SEG/USU-001-1 VALORACIÓ DE LA INFORMACIÓ I ELS SERVEIS

La informació tractada en els sistemes d'informació de la Diputació de València i els serveis als quals es destina es valoraran, a l'efecte de seguretat, atenent les cinc dimensions que comprén l'objectiu de la seguretat: disponibilitat, integritat, confidencialitat, traçabilitat i autenticitat.

Els criteris per a la valoració seran establits pel Comité de Seguretat TIC, prenent com a referència les recomanacions del Centre Criptològic Nacional, atenent com afectaria un incident de seguretat a la informació tractada o el servei per a:

a) Aconseguir els seus objectius.
b) Protegir els actius al seu càrrec.
c) Garantir la conformitat amb l'ordenament jurídic.

Les valoracions seran realitzades per cada **responsable de la Informació i del servei**, respectivament. No obstant això, podran establir-se valoracions estandarditzades de referència pel Comité de Seguretat TIC, així com proposades de valoració fetes pel responsable de Seguretat dels Sistemes d'Informació als responsables corresponents, que podran confirmar-les si les consideren adequades.

N/SEG/USU-001-2 CLASSIFICACIÓ DE LA INFORMACIÓ

Tota la informació haurà de classificar-se, en funció de les **exigències de confidencialitat**, d'acord amb els paràmetres següents:

• **Informació PÚBLICA**. Pot ser revelada o posada a la disposició del públic en general. L'accés públic pot vindre imposat o habilitat per normes legals o, simplement, per així determinar-ho els òrgans administratius competents.

• **Informació RESERVADA**. No pot ser revelada a persones alienes a la Diputació de València. És informació exclusivament d'ús intern de la corporació.

• **Informació RESTRINGIDA**. Està destinada únicament a les persones que de manera específica es determine, amb independència que aquestes persones siguen empleades de la corporació o terceres.

• **Informació CONFIDENCIAL**. Aquella accessible únicament per un reduït nombre de persones en atenció a l'especial rellevància del seu contingut, per les greus conseqüències que la seua revelació a persones més enllà del citat cercle restringit podria implicar per als interessos generals, els de la corporació o de determinades organitzacions, entitats o individus en particular.

La classificació de la informació, conforme a les categories anteriors, haurà de ser respectuosa amb el marc legal general i específic que resulte d'aplicació en cada cas.

La classificació comporta que qualsevol informació ha de fer esment al nivell al qual està adscrita, de manera que qualsevol que en pretenga fer ús conega

prèviament els límits de confidencialitat als quals s'hi troba subjecta. La informació classificada com a RESTRINGIDA i CONFIDENCIAL haurà d'indicar quines persones o entitats estan autoritzades per a accedir a aquesta.

Els qui exercisquen el rol de **responsable de la informació** —article 27 del Reglament de política de seguretat i de la protecció de dades de caràcter personal— hauran d'establir els nivells de classificació de la informació que corresponguen i determinar qui està autoritzat per a accedir-hi, i també el règim de divulgació, distribució o posada en coneixement o a l'abast de tercers.

N/SEG/USU-001-3 DEURE DE CONFIDENCIALITAT

La informació continguda o tractada en els Sistemes d'Informació de la Diputació de València és responsabilitat de la corporació, per la qual cosa els usuaris han d'abstindre's de comunicar, divulgar, distribuir o posar en coneixement o a l'abast de tercers no autoritzats (externs o interns) aquesta informació, excepte autorització expressa del **responsable de la informació** competent, en els termes exposats en l'apartat 2-001-2.

Tot el personal de l'organització o alié a aquesta que, per raó de la seua activitat professional, haguera tingut accés a qualsevol tipus d'informació gestionada per la Diputació de València haurà de mantindre sobre ella, per temps indefinit, una reserva absoluta, amb independència que la seua relació amb la corporació haja finalitzat, llevat que aquesta informació haguera sigut classificada com a PÚBLICA.

Cada **responsable de la informació** o, si s'escau, **responsable del servei**, haurà d'assegurar-se que el deure de confidencialitat i secret professional

s'establisca de manera expressa en tota mena de relacions —administratives, civils o mercantils— que impliquen o suposen accés o tractament de la informació, inclosos els serveis de simple allotjament, transport o suport tècnic, com també les conseqüències que per a la Diputació de València i per als infractors puguen derivar-se de l'incompliment d'aquests deures.

N/SEG/USU-001-4 ACCÉS I TRACTAMENT DE LA INFORMACIÓ

Tota la informació continguda o tractada en els Sistemes d'Informació de la Diputació de València o que circule per les seues xarxes de comunicacions ha de ser utilitzada únicament per al compliment de les funcions encomanades a la corporació i al seu personal.

Tot accés a la informació haurà d'estar prèviament autoritzat pel **responsable de la informació** corresponent. En compliment dels **principis de mínim privilegi i necessitat de conéixer**, els privilegis d'accés atorgats a cada usuari es reduiran al mínim estrictament necessari per a complir les seues obligacions, i es limitarà de manera que només accedisquen al coneixement d'aquella informació requerida per a complir les seues obligacions.

Haurà d'haver-hi una relació actualitzada d'usuaris i perfils d'usuaris, i els accessos autoritzats per a cadascun d'aquests.

Qualsevol accés a informació sense l'autorització citada, o amb una autorització que excedisca o no s'ajuste a l'estrictament justificat per les activitats professionals a desenvolupar, serà considerat com a accés indegut i donarà lloc a les responsabilitats corresponents.

Els usuaris que per raons del desenvolupament de la seua activitat professional tinguen accés a la informació han d'estar informats del contingut de la llei i de la normativa interna sobre la matèria, de les seues obligacions sobre aquest tema i de les conseqüències que per a ells i, si s'escau, per a la Diputació de València, implica l'incompliment de les disposicions legals i de la normativa interna.

Quan l'accés o tractament de la informació per part de tercers es fonamente en l'existència d'una prestació de serveis, **el departament o la unitat que siga responsable de la prestació de servei** a realitzar haurà d'assegurar-se del compliment de totes les garanties de seguretat de la informació recollides en la present normativa. Per això, haurà de formalitzar per escrit un document de caràcter vinculant amb el proveïdor del servei on es recullen les garanties citades, les obligacions que assumeix el proveïdor i les conseqüències del seu possible incompliment.

N/SEG/USU-001-5 EIXIDA, ARXIVAMENT I EMMAGATZEMATGE DE LA INFORMACIÓ

L'eixida d'informació de la Diputació de València (en qualsevol suport o per qualsevol mitjà de transmissió) s'haurà de realitzar exclusivament pel personal autoritzat pel **responsable de la informació** corresponent, autorització que contemplarà igualment la informació mateixa que ix.

Els usuaris s'abstindran de traure a l'exterior qualsevol informació de la Diputació de València en qualsevol dispositiu (CD, DVD, memòries USB, ordinadors o dispositius portàtils, mòbils, etc.), com tampoc transmetre-la (correu electrònic, Internet, plataformes d'intercanvi d'informació, etc.) sense comptar amb l'autorització citada en el paràgraf anterior.

Requerirà del seu xifratge, o la utilització de qualsevol altre mecanisme que garantisca que la informació no serà intel·ligible durant la seua remissió o transport, la informació classificada com a CONFIDENCIAL, qualsevol altra que així determine el responsable de la informació corresponent o el Comité de Seguretat TIC, així com quan ho determine el resultat de l'anàlisi de riscos sobre el tractament de dades de caràcter personal. Tot això sense perjudici del que es disposa en la present norma per a la informació tractada en determinats mitjans.

En l'arxivament **de la informació** s'aplicaran els criteris continguts en la present normativa, en la resta de normativa interna que puga existir sobre la matèria, com el Reglament de desenvolupament de l'administració electrònica de la Diputació de València, com també pel que es disposa en l'Esquema Nacional d'Interoperabilitat (RD 4/2010), les normes sobre patrimoni històric i arxius, i en la resta de normativa administrativa que poguera ser aplicable. En qualsevol cas, quan la informació consistisca en dades de caràcter personal el seu arxivament es farà de manera que es garantisca l'exercici dels drets d'accés, rectificació, supressió i oposició als interessats.

Amb caràcter general, **queda prohibit allotjar informació de la Diputació de València en sistemes d'informació externs**, excepte autorització expressa del Comité de Seguretat TIC que, prèvia petició del **responsable de la informació** corresponent, comprovarà la inexistència de traves legals per a fer-ho i verificarà que es poden garantir els requisits de seguretat exigibles al tipus d'informació de què es tracte. Haurà d'elaborar-se un procediment que contemple els passos a seguir per a l'obtenció de l'autorització del Comité de Seguretat TIC citada.

Els **fitxers temporals** han de ser esborrats una vegada hagen deixat de ser necessaris per als fins que van motivar la seua creació i, mentre estiguen vigents, hauran de ser emmagatzemats en la carpeta habilitada en la xarxa informàtica.

N/SEG/USU-001-6 CÒPIES DE SEGURETAT

Les còpies de suport o de seguretat garanteixen la reconstrucció de la informació davant incidents de seguretat en els quals puga veure's afectada la integritat o disponibilitat d'aquesta. Per tant, mantindre còpies de seguretat és una cautela essencial de protecció de la informació.

Correspon al Servei d'Informàtica de la corporació la realització de la còpia de seguretat periòdica de les dades allotjades en els servidors corporatius, conforme a les directrius i els procediments que establisca el Comité de Seguretat TIC.

Tota la informació de la Diputació de València ha de guardar-se en les unitats de xarxa assignades, de manera que se'n garantisca l'entrada en els processos de còpia de seguretat sistemàtics de les dades. Les dades generades pels usuaris en l'acompliment de les seues competències professionals hauran de mantindre's en un repositori únic, en la unitat de xarxa compartida que designe el Servei d'Informàtica.

N/SEG/USU-001-7 ANÀLISI I GESTIÓ DE RISCOS

L'anàlisi de riscos, entesa com la utilització sistemàtica de la informació disponible per a identificar perills i estimar els riscos, resulta fonamental per a una gestió adequada de la seguretat dels sistemes d'informació.

En compliment de l'article 12 del Reglament de política de seguretat i de la protecció de dades de caràcter personal, tots els sistemes d'informació hauran de realitzar una anàlisi de riscos, avaluant les amenaces i els riscos als quals estan exposats:

- Regularment, almenys una vegada a l'any
- Quan canvie la informació manejada
- Quan canvien els serveis prestats
- Quan ocórrega un incident greu de seguretat
- Quan es reporten vulnerabilitats greus

Els criteris per a l'anàlisi i la metodologia a aplicar seran establits per la normativa de seguretat aplicable al personal tècnic dels sistemes d'informació TIC, i aquesta anàlisi és la base per a determinar les mesures de seguretat que s'han d'adoptar, a més dels mínims establits en l'Esquema Nacional de Seguretat.

Haurà d'establir-se un procediment amb les pautes a seguir per a dur a terme l'anàlisi i la gestió de riscos dels sistemes d'informació. Per a l'harmonització de les anàlisis, el Comité de Seguretat TIC podrà establir una valoració de referència per als diferents tipus d'informació manejats i els diferents serveis prestats.

N/SEG/USU-002 SEGURETAT DELS MITJANS TECNOLÒGICS IMPLICATS EN EL TRACTAMENT DE LA INFORMACIÓ

Tots els mitjans tecnològics posats a la disposició dels usuaris: ordinadors personals i portàtils, aplicacions, programes, sistemes d'impressió i escaneig de documents, dispositius mòbils, l'accés a la xarxa corporativa i a Internet, són propietat de la Diputació de València, i són elements molt importants en la

cadena de seguretat dels sistemes d'informació, raó per la qual és necessari adoptar una sèrie de precaucions i establir normes per a la seua utilització adequada.

En el present apartat es recullen les normes d'ús degut que tots els usuaris hauran d'observar en la utilització dels mitjans tecnològics que la corporació posa a la seua disposició.

N/SEG/USU-002-1 UTILITZACIÓ DELS MITJANS TECNOLÒGICS

La Diputació de València facilitarà als usuaris que ho necessiten els mitjans citats per al desenvolupament de la seua activitat professional, és a dir, per a les funcions encomanades, per la qual cosa **qualsevol ús dels recursos amb finalitats diferents als autoritzats està estrictament prohibit**.

La configuració i instal·lació dels mitjans tecnològics es reserva exclusivament al personal tècnic del Servei d'Informàtica de la Diputació de València.

No està permés:

• Alterar la configuració hardware dels equips ni connectar altres dispositius a aquests a iniciativa de l'usuari, com tampoc variar la seua ubicació.

• Alterar la configuració software dels equips, desinstal·lar o instal·lar programes diferents a la configuració establida pel Servei d'Informàtica de la Diputació de València.

• La instal·lació, utilització o connexió a la xarxa corporativa de qualsevol mitjà tecnològic diferent dels admesos, habilitats i configurats pel Servei d'Informàtica de la Corporació sense comptar amb la deguda autorització d'aquest Servei.

• Emmagatzemar informació privada, de qualsevol naturalesa, en els ordinadors personals i en els recursos d'emmagatzematge compartits.

N/SEG/USU-002-2 INFORMACIÓ EN ESPAIS O PLATAFORMES D'INTERNET

Tots els espais i plataformes en Internet o tecnologies similars la titularitat de les quals corresponga a la corporació, o que s'utilitzen en nom de la Diputació de València, **hauran de complir els requisits de seguretat tècnica i jurídica** exigits per la Llei i per la normativa interna.

A fi d'assegurar el compliment degut dels requisits de seguretat citats, s'establirà un procediment que contemple la mecànica a seguir pels diferents departaments que pretenguen fer ús d'aquests entorns, de manera que es garantisca la supervisió prèvia del responsable de Seguretat dels Sistemes d'Informació.

Queda prohibit posar en servei o utilitzar en nom de la Diputació de València qualsevol dels espais tecnològics referits sense que complisquen els requisits esmentats.

N/SEG/USU-002-3 NORMES ESPECÍFIQUES PER A DISPOSITIUS PORTÀTILS I MÒBILS

A l'efecte d'aquest apartat s'entén per dispositiu mòbil els ordinadors portàtils, les tauletes, telèfons mòbils tradicionals i intel·ligents (*smartphones*), lectors de llibres electrònics (*e-readers*), claus electròniques, USB, DVD i similars.

Els dispositius portàtils i mòbils que resulten necessaris per a l'acompliment de l'activitat professional seran posats a la disposició dels usuaris per la Diputació de València. **Està prohibit utilitzar dispositius portàtils i mòbils no proporcionats per la corporació per a emmagatzemar, accedir, transmetre o tractar de qualsevol altra manera informació**, excepte si es compta amb l'autorització a què es fa referència més endavant.

Prèviament a la seua entrega o posada en servei, **els dispositius hauran de ser objecte d'una configuració de seguretat per defecte**, que serà realitzada pel Servei d'Informàtica conforme a la naturalesa del dispositiu i seguint les directrius que s'establisquen en la normativa de seguretat dirigida al personal TIC i les que puga fixar el Comité de Seguretat TIC.

La configuració de seguretat podrà limitar o restringir la connexió directa a xarxes externes, els canals, ports i sistemes de comunicacions d'eixida d'informació (Wifi, Bluetooh, USB, CD, DVD, targetes de xarxa, etc.), com també la instal·lació i execució de programari (app, etc.) i els serveis que seran accedits (e-mail, VPN, CRM…).

La Diputació de València tindrà la potestat, en qualsevol cas, igual que per a la resta de mitjans tecnològics posats a la disposició del seu personal, del monitoratge, l'esborrament remot de dades o la realització d'auditories de seguretat sobre aquests dispositius.

Per defecte, i amb caràcter general, els dispositius esmentats es configuraran per a mantindre xifrades les dades i informacions que puguen emmagatzemar, així com les transmissions d'informació que, si s'escau, puguen autoritzar-se. Podrà excloure's d'aquesta mesura aquella informació que estiga classificada com a PÚBLICA.

En el moment de posar els dispositius a disposició dels usuaris, aquests hauran d'haver sigut configurats perquè incorporen aquelles mesures de seguretat suficients per a assegurar la protecció de la informació al llarg de tot el cicle de vida del dispositiu.

Hi haurà un **inventari actualitzat dels equips portàtils i mòbils** que permeta la identificació personalitzada de cada dispositiu, saber a qui i quan es fa entrega d'aquest, les incidències que l'afecten (robatori, pèrdua, reparació, etc.), així com la seua baixa operativa i la seua destinació després d'aquesta. Aquest inventari serà portat pel Servei d'Informàtica de la Corporació.

En principi, els dispositius portàtils i mòbils hauran d'utilitzar-se únicament per a fins professionals, no per a fins privats. No obstant això, podrà ser autoritzat un ús per als dos fins quan es donen les circumstàncies següents:

a) Que la corporació dispose de productes tecnològics que permeten segregar les dues àrees d'activitat en els dispositius i garantir la incomunicabilitat entre elles, de manera que quede salvaguardat el dret a la privacitat sense perjudici del compliment de totes les normes de seguretat establides per la Diputació i les potestats de gestió i control que aquesta ostenta.

b) Que l'usuari, degudament informat, accepte expressament aquestes condicions d'ús.

Sense perjudici de les directrius establides sobre l'ús en general dels mitjans tecnològics (2-002-1), seran aplicables als dispositius portàtils i mòbils les següents:

• Aquest tipus de dispositius estaran sota la custòdia de l'usuari que els utilitze, el qual haurà d'adoptar les mesures necessàries per a evitar danys o sostracció, com també l'accés a aquests per part de persones no autoritzades.

• La pèrdua o sostracció d'aquests dispositius s'haurà de posar immediatament en coneixement del Servei d'Informàtica de la Corporació, per a l'adopció de les mesures que corresponguen i a l'efecte de baixa en l'inventari.

• Els usuaris d'aquests dispositius hauran de realitzar connexions periòdiques a la xarxa corporativa, segons les instruccions proporcionades pel Servei d'Informàtica, per a permetre l'actualització d'aplicacions, sistema operatiu, signatures d'antivirus i altres mesures de seguretat.

• Quan es modifiquen les circumstàncies professionals (acabament d'una tasca, canvi de lloc o funcions, cessament en el càrrec, etc.) que van originar el lliurament d'un recurs informàtic mòbil, l'usuari el retornarà al Servei d'Informàtica de la corporació, a fi de procedir a l'esborrament segur de la informació hi emmagatzemada i, si s'escau, restaurar l'equip al seu estat original perquè puga ser assignat a un nou usuari.

Podran utilitzar-se **dispositius portàtils o mòbils no proporcionats per la Diputació de València** per a emmagatzemar, accedir, transmetre o tractar de

qualsevol altra manera informació, únicament quan concórrega algun dels supòsits següents:

a) Es tracte d'una necessitat professional **excepcional, específica i per temps molt limitat**.

b) Que la informació a tractar s'haja classificat com a PÚBLICA.

c) Es tracte dels supòsits de teletreball indicats en la norma 2-002-11, apartat b, de la present normativa.

La utilització dels dispositius en aquests casos haurà d'estar expressament autoritzada pel Responsable de la Informació corresponent, el qual ho comunicarà al Comité de Seguretat TIC, i a més hauran de complir-se, en el supòsit de l'apartat a), els requisits següents:

- En cap cas no es podrà tractar d'informació classificada com a CONFIDENCIAL o quan així ho determine el resultat de l'anàlisi de riscos sobre el tractament de dades de caràcter personal.
- L'autorització contindrà la motivació i el marc temporal de la necessitat.
- El dispositiu haurà de proporcionar l'entorn de seguretat que resulte exigible, i podrà ser comprovat pel Servei d'Informàtica.
- L'usuari/propietari estarà sotmés a les mateixes obligacions de custòdia i de connexions periòdiques, i hi haurà acceptació per la seua part de les condicions d'ús,

que les descrites anteriorment per als usuaris de dispositius autoritzats per a fins professionals i privats.

N/SEG/USU-002-4 SUPORTS ELECTRÒNICS D'INFORMACIÓ

A l'efecte d'aquest apartat s'entén per suports electrònics d'informació els DVD, CD, USB (*pen drives*), discos durs externs, targetes de memòria (SD, UFC, SM, MMS, etc.), claus intel·ligents o electròniques, cintes magnètiques i qualsevol altre suport similar diferent dels dispositius indicats en l'apartat 2-002-3.

Per raons de seguretat, les interfícies dels llocs d'usuari que connecten aquests suports estaran deshabilitades. En cas que siga necessari, el **responsable de la informació** corresponent sol·licitarà al Servei d'Informàtica una solució adequada que atenga aquesta necessitat.

Els suports electrònics d'informació que resulten necessaris per a l'acompliment de l'activitat professional seran posats a la disposició dels usuaris per la Diputació de València. **Està prohibit utilitzar suports electrònics d'informació no proporcionats per la Corporació per a emmagatzemar informació**, excepte si es tracta d'informació classificada com a PÚBLICA i es compta amb l'autorització del responsable de la informació corresponent.

Cada departament serà responsable de la determinació del tipus de suport a utilitzar i de la seua gestió (etiquetatge, inventari, registre, distribució, custòdia, esborrament i destrucció) conforme a les especificacions següents:

a) **Etiquetatge**. Tots els suports d'informació hauran de ser etiquetats mitjançant un sistema que permeta, només al personal autoritzat,

identificar el tipus d'informació que contenen, i el nivell de classificació i de seguretat d'aquesta.

b) Inventari. Tots els suports d'informació seran inventariats, de manera que puguen ser identificats singularment. L'inventari recollirà, com a mínim, les dades del cicle vital de cada suport (alta, incidències, baixa).

c) Registre. Haurà de portar-se un registre actualitzat d'entrada i eixida de suports d'informació. El registre reflectirà, com a mínim, el tipus de suport, la data i l'hora, l'emissor i el destinatari, el nombre de suports inclosos en l'enviament, el tipus d'informació que contenen, la forma d'enviament i la persona responsable de la recepció i del lliurament, respectivament, que haurà d'estar degudament autoritzada.

d) Custòdia. S'aplicarà la deguda diligència i control als suports d'informació que romanen sota la responsabilitat de cada departament, mitjançant les actuacions descrites en l'apartat 2-003-3, i garantirà que es respecten les exigències de manteniment del fabricador, especialment referent a temperatura, humitat i altres agressors mediambientals. No obstant això, si es produïra la sostracció, pèrdua o accés indegut als suports d'informació s'haurà de posar en coneixement del responsable de Seguretat dels Sistemes d'Informació, a través del sistema de notificació d'incidències de seguretat.

e) Transport. En el trasllat de suports d'informació s'adoptaran les mesures pertinents per a evitar la sostracció, la pèrdua o l'accés indegut a la informació durant el seu transport, especialment quan la informació continguda en el suport no haja sigut objecte de xifratge. Es disposarà d'un procediment rutinari que acare les eixides amb les arribades i alce

les alarmes pertinents quan es detecte algun incident. En cas de sostracció, pèrdua o accés indegut a la informació durant el seu transport s'haurà de posar en coneixement del responsable de Seguretat dels Sistemes d'Informació, a través del sistema de notificació d'incidències de seguretat.

N/SEG/USU-002-5 ESBORRAMENT I DESTRUCCIÓ DE SUPORTS ELECTRÒNICS D'INFORMACIÓ

El Servei d'Informàtica procedirà a l'esborrament segur i destrucció dels suports d'informació, inclosos els dispositius portàtils i mòbils, com també de qualsevol altre sobre el qual es puguen gravar i recuperar dades, que utilitzen els diferents departaments de la Diputació de València, i podrà també posar a la disposició dels usuaris departamentals eines d'esborrament segur dels seus suports d'informació. A aquests efectes, s'haurà de disposar d'un procediment per a l'esborrament segur i la destrucció de suports d'informació.

Està prohibit reutilitzar i rebutjar suports d'informació sense que prèviament hagen sigut objecte de l'eliminació permanent de la informació que pogueren contindre, de manera que resulte impossible la seua recuperació ni tan sols de manera parcial.

N/SEG/USU-002-6 ÚS DEL CORREU ELECTRÒNIC

El **correu electrònic corporatiu** és una eina de missatgeria electrònica centralitzada, posada a la disposició dels usuaris de la Diputació de València, per a l'enviament i la recepció de correus electrònics mitjançant l'ús de comptes de correu corporatius.

La utilització del correu electrònic com a eina de treball s'ajustarà a les normes generals següents:

• Tots els usuaris que ho necessiten per a l'acompliment de la seua activitat professional disposaran d'un compte de correu electrònic per a l'enviament i la recepció de missatges interns i externs a l'organització.

• Únicament podran utilitzar-se les eines i els programes de correu electrònic subministrats, instal·lats i configurats pel Servei d'Informàtica de la Diputació de València.

• El correu corporatiu haurà d'utilitzar-se, exclusivament, per a la realització de les funcions encomanades al personal, evitant-ne l'ús privat.

• El correu corporatiu serà l'única eina de correu electrònic que haurà d'utilitzar-se per als assumptes professionals.

• Per a verificació i monitoratge, les dades de connexió i trànsit es guardaran en un registre durant el temps que establisca la normativa vigent en cada supòsit. En cap cas aquesta retenció de dades afectarà el secret de les comunicacions.

• El correu corporatiu no serà utilitzat per a l'intercanvi de fitxers excepte en aquells supòsits en què així es permeta, tal com es recull en la norma N/SEG/USU-002-10.

N/SEG/USU-002-7 ÚS D'INTERNET

L'**accés corporatiu a Internet** és un recurs centralitzat que la Diputació de València posa a la disposició dels usuaris, com a eina necessària per a l'accés a continguts i recursos d'Internet i com a suport a l'acompliment de la seua activitat professional.

L'accés a Internet haurà de ser autoritzat pel responsable del departament o la unitat administrativa, seguint el procediment intern que es determine, sempre que s'estime necessari per a l'acompliment de l'activitat professional de l'usuari o sol·licitant, i hi haja disponibilitat per a això. En un altre cas, es podrà accedir a Internet des d'un lloc d'accés comú habilitat per a aquest fi.

Tindrà la consideració d'ús professional d'internet l'accés a activitats formatives reglades a les quals el personal tinga dret i/o autorització en el marc de la normativa legal o interna, que requerisquen la utilització d'aquest recurs i que es duguen a terme durant el temps de treball.

Només es podrà accedir a Internet mitjançant els navegadors subministrats i configurats pel Servei d'Informàtica en els llocs d'usuari. No se'n podrà alterar la configuració ni utilitzar un navegador alternatiu sense la autorització deguda del Servei d'Informàtica.

La utilització d'Internet ha d'obeir a fins professionals, tenint sempre en compte que s'estan utilitzant recursos informàtics restringits i escassos. L'accés a Internet per a fins personals tindrà caràcter extraordinari, se n'haurà de limitar la utilització dins d'un temps raonable que no interferisca en el rendiment professional ni en l'eficiència dels recursos informàtics corporatius.

La Diputació de València vetlarà pel bon ús de l'accés a Internet, tant des del punt de vista de l'eficiència i productivitat del personal com des dels riscos de seguretat associats al seu ús. En aquest sentit, sota els criteris establits pel Comité de Seguretat TIC, podran implementar-se eines que restringisquen o limiten els accessos a determinats continguts, categories de pàgines web, ubicacions o les accions dels usuaris (descàrregues, instal·lació de components, execució de determinat programari, etc.). D'igual forma, podran establir-se diferents nivells d'accés dels usuaris, segons la necessitat d'utilització d'Internet d'aquests.

N/SEG/USU-002-8 ÚS D'IMPRESSORES, FOTOCOPIADORES, ESCÀNERS I FAXOS

Amb caràcter general, hauran d'utilitzar-se les impressores en xarxa i les fotocopiadores corporatives. Excepcionalment podran instal·lar-se impressores locals, gestionades per un lloc de treball d'usuari. En aquest cas, la instal·lació anirà precedida de l'autorització pertinent per part del responsable del peticionari.

Quan s'imprimisca, fotocopie, digitalitze o es remeta per fax documentació, haurà de romandre el menor temps possible en les safates d'eixida dels equips implicats, per a evitar que terceres persones puguen accedir a aquesta. Convé no oblidar retirar els originals de la fotocopiadora, impressora, escàner o fax una vegada finalitzat el procés corresponent. Si es trobara documentació

abandonada en una fotocopiadora, impressora, escàner o fax, l'usuari intentarà localitzar el seu propietari perquè aquest la reculla immediatament. En cas que es desconega el propietari o no es localitze, es posarà immediatament en coneixement del superior jeràrquic.

Amb caràcter general, quan es digitalitzen documents, l'usuari haurà de ser especialment acurat amb la selecció del directori compartit on hauran d'emmagatzemar-se les imatges obtingudes, especialment si contenen informació no classificada com a PÚBLICA.

Sense perjudici de les pautes descrites anteriorment per als usuaris, el Servei d'Informàtica haurà d'elaborar rutines automatitzades per a l'esborrament periòdic de la informació que puga quedar emmagatzemada en les carpetes, directoris o memòria dels dispositius o recursos compartits per a la fotocòpia, impressió, escanejat o transmissió per fax.

N/SEG/USU-002-9 CONTROL D'ACCESSOS ALS SISTEMES D'INFORMACIÓ

Correspon al Servei d'Informàtica de la Corporació establir els diferents mecanismes que garantisquen l'accés a les xarxes, les aplicacions i les dades únicament als usuaris i processos degudament autoritzats. La naturalesa dels mecanismes citats serà la que resulte més adequada en funció dels requisits de seguretat específics per a cada cas, en virtut de les directrius fixades per a això pel Comité de Seguretat TIC.

Haurà d'elaborar-se un procediment que establisca les pautes a seguir per a la petició d'accés d'usuaris als sistemes d'informació, així com per a la baixa i eliminació efectiva dels drets d'accés.

Els mecanismes que es posen a la disposició dels usuaris per a la seua deguda identificació i autenticació en els sistemes d'informació podran consistir en claus concertades, contrasenyes, targetes d'identificació o qualsevol altre dispositiu físic (*tokens*) o components lògics (certificat de programari), mecanismes biomètrics o qualssevol altres de naturalesa anàloga.

Aquests mecanismes seran personals i intransferibles, i hauran de proporcionar una identificació individual i inequívoca. Els usuaris són responsables de la custòdia d'aquests i de tota activitat relacionada amb l'ús del seu accés autoritzat, per la qual cosa no hauran de revelar o entregar en cap cas, en cap concepte, els seus mecanismes de credencials d'accés a terceres persones, ni tan sols a altres usuaris o personal al servei de la Diputació de València, ni mantindre'ls per escrit a la vista o a l'abast de tercers. Els usuaris no han d'utilitzar cap accés autoritzat d'un altre usuari, encara que disposen de l'autorització del seu titular.

Si un usuari té sospites que les seues credencials estan sent utilitzades per una altra persona, ha de procedir immediatament a comunicar la **incidència de seguretat** corresponent. De la mateixa manera, haurà d'actuar-se quan es produïsca la pèrdua o l'extraviament del mecanisme, un mal funcionament o qualsevol altre comportament anòmal d'aquest.

S'establiran les mesures necessàries per a limitar el nombre d'intents d'accés fallits als sistemes d'informació, de manera que, una vegada superat aquest, es produirà el bloqueig automàtic de l'usuari. D'igual forma, quan s'utilitzen

contrasenyes hauran d'incorporar-se mesures que forcen l'usuari al canvi periòdic d'aquestes. El límit d'intents d'accés fallits, la periodicitat per al canvi de contrasenyes i la política de qualitat d'aquestes seran determinats pel Comité de Seguretat TIC.

Haurà d'elaborar-se un procediment per a l'assignació, distribució i emmagatzematge, si s'escau, dels mecanismes utilitzats per a la identificació i l'autenticació en els sistemes d'informació.

N/SEG/USU-002-10 INTERCANVI DE FITXERS

Únicament es procedirà a la remissió de fitxers mitjançant les aplicacions i els canals que determine el Servei d'Informàtica, de manera que quede garantida la seguretat, confidencialitat i traçabilitat de la informació transmesa. Utilitats com el correu electrònic corporatiu, entorns FTP i altres en manera núvol —drive, icloud, Dropbox, etc.— o similar, **no s'utilitzaran per a l'intercanvi de fitxers,** llevat que es tracte d'informació classificada com a PÚBLICA o hi haja una autorització expressa del Servei d'Informàtica.

Quan l'intercanvi de fitxers es produïsca en ocasió de la prestació de serveis contractats per la Diputació de València, el servei responsable imposarà al proveïdor el canal d'intercanvi segons l'indicat en el paràgraf anterior. En els instruments vinculants de contractació es farà constar aquesta circumstància, i haurà de constituir una condició obligatòria de la prestació.

Si l'intercanvi de fitxers és conseqüència de l'assistència de la Diputació de València a les entitats locals es procedirà d'igual manera. El Servei responsable d'aquesta assistència comunicarà la circumstància a l'Entitat Local receptora de

l'assistència, i informarà del seu caràcter obligatori per al desenvolupament de l'assistència. Sempre que hi haja un instrument administratiu que regule o reculla els termes de l'assistència —conveni, acord, etc.— s'hi haurà de fer constar aquesta circumstància.

En aquells supòsits de col·laboració administrativa o percepció de prestacions d'altres entitats públiques en els quals la Diputació de València no puga imposar aquestes condicions per a l'intercanvi de fitxers, s'intentarà que aquestes entitats accepten el canal proposat per la Diputació almenys per a la remissió dels fitxers per part de la Diputació, sempre que siga possible.

Les aplicacions i els canals que hagen de determinar-se pel Servei d'Informàtica per a l'intercanvi de fitxers seran consensuats prèviament en el si del Comité de Seguretat TIC.

N/SEG/USU-002-11 MODALITAT DE TELETREBALL

Quan es duga a terme la prestació de serveis en la modalitat de teletreball a l'empara del Reglament de prestació de serveis mitjançant teletreball (sector no sanitari), aprovat per acord del Ple de la corporació de 23 de novembre de 2021, s'aplicaran les regles següents:

a) En el cas de teletreball derivat de necessitats organitzatives, com també en aquells supòsits recollits en el capítol IV del citat reglament de teletreball —Altres modalitats d'accés al teletreball— en què al personal afectat se li facilite l'equipament informàtic i les aplicacions informàtiques per part de la Diputació, s'aplicaran les mateixes regles de seguretat de la informació contingudes en les presents normes de seguretat per als

usuaris dels sistemes d'informació, i també les singularitats recollides en el reglament de teletreball, especialment:

▪ Que 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 la delegació que tinga atribuïdes les competències en informàtica i noves tecnologies.

▪ Que l'equipament informàtic i les aplicacions informàtiques subministrades seran d'ús exclusivament laboral.

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

▪ Que correspondrà a l'empleat o empleada la comunicació de les incidències que puguen produir-se en l'equip informàtic. En el supòsit de produir-se deficiències o desperfectes derivats d'un ús inadequat o negligent, la Diputació podrà exigir les responsabilitats oportunes a l'empleat o empleada corresponent.

▪ Que 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 ocorregueren o el següent, 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.

b) En els supòsits restants de teletreball, diferents als indicats en l'apartat a), en els quals els dispositius i/o elements informàtics utilitzats siguen per compte de la persona teletreballadora, serà aplicable el que es disposa per als **dispositius mòbils no proporcionats per la Diputació de València** en la norma 2-002-3 Normes específiques per a dispositius portàtils i mòbils, com també les regles de seguretat singulars que puguen determinar-se pel Servei d'Informàtica en cada cas concret.

En tots els supòsits de prestació del servei mitjançant la modalitat de teletreball podran establir-se mesures de seguretat complementàries o diferents a les previstes en la normativa interna de seguretat de la informació, quan així ho aconselle el resultat de l'avaluació de riscos. En aquests supòsits, el personal afectat serà informat degudament de les citades mesures i vindrà obligat al seu compliment.

N/SEG/USU-003 SEGURETAT D'ALTRES ACTIUS DELS SISTEMES D'INFORMACIÓ

N/SEG/USU-003-1 SEGURETAT DE LOCALS I 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. Les condicions de seguretat que han de reunir aquests recintes seran establides en la normativa de seguretat dirigida al personal TIC.

Els locals que s'utilitzen per a l'atenció al públic evitaran situar en les zones accessibles a aquest, o en zones de pas, elements dels sistemes d'informació com ara impressores, faxos, fotocopiadores, arxivadors, etc.

Sempre que resulte possible, els locals es distribuiran de manera que els llocs de treball se situen atenent uns mateixos privilegis d'accés a la informació o similars, així com a l'ús de recursos compartits.

N/SEG/USU-003-2 SEGURETAT A L'ENTORN DE TREBALL

Els llocs de treball romandran espaiosos, sense més material damunt la taula que el requerit per a l'activitat que s'està realitzant a cada moment. Aquella documentació que no s'haja d'utilitzar en el moment haurà de guardar-se en calaixos sota clau o en els armaris o arxivadors corresponents.

Qualsevol usuari que s'absente temporalment del seu lloc de treball haurà de bloquejar la sessió del seu ordinador (estalvis de pantalla amb contrasenya, etc.) per a impedir l'accés d'altres persones a la informació i a l'equip informàtic. S'establiran bloquejos de sessió automàtics per temps d'inactivitat, i es requerirà una nova autenticació de l'usuari per a reprendre l'activitat en curs.

Al final de la jornada de treball, els usuaris hauran d'assegurar-se que l'equip està apagat i que no es deixa accessibles documentació ni suports d'informació de cap mena.

Quan s'utilitzen pissarres i *flipcharts,* els usuaris hauran d'assegurar-se que es netegen adequadament, perquè no quede cap mena d'informació a la vista,

abans d'abandonar les sales o despatxos on se situen o permetre que algú alié entre.

El menjar i la beguda poden danyar tant els components electrònics com els suports d'informació, per la qual cosa no hauran de realitzar-se aquestes accions en el lloc de treball, llevat que s'adopten totes les garanties que impedisquen el risc de mal esmentat.

N/SEG/USU-003-3 ARXIVADORS I RECINTES DEDICATS A L'EMMAGATZEMATGE D'INFORMACIÓ

Els armaris, arxivadors o altres elements en els quals se situen els suports d'informació hauran de disposar de mecanismes de tancament que impedisquen l'accés a persones no autoritzades.

Sempre que siga possible, aquests armaris o arxivadors han de trobar-se en àrees en les quals l'accés estiga protegit amb portes d'accés dotades de sistemes d'obertura mitjançant clau o un altre dispositiu equivalent. Aquestes àrees hauran de romandre tancades quan no calga l'accés als suports d'informació que contenen.

Haurà d'evitar-se l'emmagatzematge, depòsit o arxivament de suports d'informació en recintes o armaris d'ús comú, llevat que es garantisca l'existència de mecanismes que facen possible l'accés a la informació únicament al personal autoritzat en cada cas.

Las dependències destinades a l'arxiu d'informació no s'utilitzaran per a altres usos, com el de magatzem de papereria, d'utensilis informàtics, material de neteja, taquilles i vestidors, o qualsevol altra utilitat que supose l'accés a aquests

recintes de personal diferent a l'autoritzat per a accedir a la informació emmagatzemada.

Aquestes dependències disposaran de les garanties mediambientals degudes que impedisquen qualsevol mal o deterioració dels suports d'informació, i també de mecanismes de detecció i extinció d'incendis adequats al tipus de suports que continguen.

N/SEG/USU-003-4 INFORMACIÓ EN SUPORTS NO AUTOMATITZATS

Tota la informació en suports no automatitzats (documents en paper, carpetes, expedients, dossiers, etc.) haurà de situar-se en armaris, arxivadors i recintes amb les característiques que s'estableixen en l'apartat 2-003-3.

Mentre la documentació no es trobe arxivada en els dispositius d'emmagatzematge citats, per estar en procés de revisió o tramitació, ja siga previ o posterior al seu arxivament, la persona que se'n trobe al càrrec l'haurà de custodiar i impedir en tot moment que puga ser accedida per persona no autoritzada.

Sense perjudici del que puga establir la normativa sobre procediment administratiu que en cada cas resulte d'aplicació, quan es tracte de documentació que continga informació classificada com a CONFIDENCIAL o quan el determine el resultat de l'anàlisi de riscos sobre el tractament de dades de caràcter personal**,** s'establiran mecanismes que permeten identificar els accessos realitzats en el cas de documents que puguen ser utilitzats per múltiples usuaris.

La generació de còpies o la reproducció dels documents únicament podrà dur-se a terme sota el control del personal autoritzat. Les còpies de documents que s'hagueren creat exclusivament per a la realització de treballs temporals o auxiliars estaran subjectes als mateixos requisits de seguretat que els documents originals, i hauran de ser destruïdes una vegada hagen deixat de ser necessàries per als fins que van motivar la seua creació.

La destrucció dels documents que continguen informació no classificada com a PÚBLICA, incloses les còpies o reproduccions, es realitzarà mitjançant màquines destructores, de manera que s'evite la recuperació o reconstrucció de la informació amb posterioritat.

Sempre que es procedisca al trasllat físic de documents que continguen informació no classificada com a PÚBLICA, hauran d'adoptar-se mesures dirigides a impedir l'accés o la manipulació de la informació objecte de trasllat.

N/SEG/USU-004 AUDITORIES DE SEGURETAT

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.

b) Auditories reglamentàries, regulars o extraordinàries, en compliment de l'Esquema Nacional de Seguretat. L'objecte d'aquestes auditories de la seguretat, internes o externes, és el contingut en l'article 31 de l'Esquema Nacional de Seguretat, el qual determina que els sistemes d'informació seran objecte d'una auditoria regular ordinària, almenys cada dos anys, que verifique el compliment dels requeriments de l'Esquema Nacional de Seguretat; i també que, amb caràcter extraordinari, haurà de realitzar-se aquesta auditoria sempre que es produïsquen modificacions substancials en els sistemes d'informació, que puguen repercutir en les mesures de seguretat requerides. Són auditories obligatòries i de caràcter reglamentari.

Els informes de resultats de les auditories periòdiques de seguretat 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. 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 esmentat.

Els informes d'auditoria seran analitzats pel responsable de Seguretat dels Sistemes d'Informació i pel Departament de Protecció de Dades i Seguretat de la Informació, que presentaran les seues conclusions al Comité de Seguretat TIC perquè adopte les mesures correctores adequades.

En el cas dels sistemes crítics i de categoria ALTA, vist el dictamen d'auditoria, el responsable dels sistemes d'Informació podrà acordar la retirada d'operació

d'alguna informació, d'algun servei o del sistema íntegrament, durant el temps que estime prudent i fins a la satisfacció de les modificacions prescrites.

Tots els empleats de la corporació estan obligats a facilitar tota la informació que els siga requerida pel personal que duga a terme les auditories recollides en el present apartat, així com l'accés a locals, instal·lacions, equips, arxius, suports d'emmagatzematge, programes, processos i procediments.

N/SEG/USU-005 NORMES ESPECIALS PER A VÍDEOVIGILÀNCIA

Els equips informàtics utilitzats per a la captació, l'emmagatzematge i el processament de les imatges i sons amb finalitats de videovigilància hauran de tindre les característiques següents:

• No seran utilitzats per a cap tasca diferent de la de videovigilància, per la qual cosa l'únic programari que contindran serà el necessari per a aquesta funció.

• Es configuraran de manera que, excepte els mecanismes de transmissió de la informació amb el centre de processament de dades, es troben inhabilitades les possibilitats de connexió amb xarxes externes i l'entrada-eixida d'informació (Wifi, Bluetooth, USB, CD, DVD, etc.).

• Preferentment, els equips locals no emmagatzemaran la informació recaptada, sent recomanable que aquesta es transmeta al centre de processament de dades remot. Si les circumstàncies tècniques impediren o feren molt onerosa aquesta transmissió, podran habilitar-se dispositius d'emmagatzematge local autònoms (diferents al disc dur integrat en l'equip local des del qual es gestionen els elements de captació de les imatges) sempre que estiguen situats en recintes

amb control d'accés restringit i disposen de mecanismes d'autenticació per a l'accés a la informació.

• L'accés o l'inici de sessió al sistema estarà protegit per un mecanisme d'autenticació que identifique qui hi accedeix i només permeta l'accés a usuaris autoritzats. El **protocol d'actuació en matèria de videovigilància** descrit en la norma N/PDP-014 contindrà les especificacions que haurà de tindre el mecanisme d'autenticació.

• Els equips estaran fora de l'abast del personal no autoritzat. Sempre que les característiques de les instal·lacions i del servei ho permeten, s'habilitarà un recinte tancat i independent per a la ubicació dels equips informàtics locals de videovigilància que facilite el control d'accés a persones no autoritzades. En cas de no disposar d'aquest recinte, els equips se situaran en llocs sota el control permanent del personal de vigilància i es disposaran de manera que les imatges no puguen ser visualitzades per tercers.

Per a garantir que l'accés als sistemes, a les dades i als suports que els continguen es limita al personal autoritzat que determina la norma N/PDP-014-3, el personal adscrit al servei de vigilància dels locals i les instal·lacions de la Diputació de València serà responsable d'impedir que el personal no autoritzat:

- Accedisca físicament als recintes on se situen els equips informàtics, en cas que hi haja recintes amb aquesta funció.
- Accedisca a imatges i/o sons recollits, encara que siga en temps real.
- Manipule de qualsevol forma els equips i suports informàtics.

Es disposarà d'un **centre de control** en el qual s'emmagatzemaran tots els enregistraments generats pels sistemes de videovigilància de la Diputació de València. Aquest centre serà el responsable de:

- Mantindre les condicions de seguretat de les dades i dels suports que les continguen.
- Proporcionar a la Diputació de València les dades de què dispose quan li siga requerit per aquesta a través del personal degudament autoritzat.
- Assegurar la transmissió de les dades des dels terminals locals de videovigilància als servidors del centre.

Les condicions específiques de seguretat que ha de reunir el centre de control seran establides en el **protocol d'actuació en matèria de videovigilància**, atesos la normativa de seguretat de la informació de la Corporació i els riscos als quals a cada moment s'estiga exposat. D'igual manera, en el protocol citat s'especificaran els terminis de manteniment de la informació i el procediment per a proporcionar dades a requeriment de la Diputació de València.

N/SEG/USU-006 INCIDENTS DE SEGURETAT

Haurà d'elaborar-se un procediment general que establisca les pautes d'actuació dels usuaris dels sistemes d'informació davant incidents que puguen afectar la seguretat de la informació. Aquest procediment inclourà, en qualsevol cas, les vies per a notificar les incidències i la informació requerida.

N/SEG/USU-006-1 NOTIFICACIÓ D'INCIDÈNCIES

És obligació de qualsevol usuari comunicar totes aquelles incidències de seguretat que es produïsquen en l'àmbit dels sistemes d'informació. Les incidències seran reportades al responsable de Seguretat dels Sistemes d'Informació per a la seua gestió corresponent i posterior informació, si s'escau, al Comité de Seguretat TIC.

S'habilitarà un mecanisme electrònic per a la comunicació d'incidències. D'igual manera, s'implementaran sistemes de detecció i notificació automàtica d'incidències.

N/SEG/USU-006-2 REGISTRE D'INCIDÈNCIES

Totes les incidències que es comuniquen o notifiquen quedaran registrades. Aquest registre s'ajustarà, com a mínim, al següent:

a) Es registrarà el report inicial, les actuacions d'emergència i les modificacions del sistema derivades de l'incident.

b) Es registraran aquelles evidències que puguen, posteriorment, sustentar una demanda judicial, o fer-li front, quan l'incident puga portar a actuacions disciplinàries sobre el personal intern, sobre proveïdors externs o a la persecució de delictes.

En el cas que la incidència puga afectar dades personals, a més, en virtut de l'article 33.3 RGPD, en aquest registre haurà de constar:

a) Descripció de la naturalesa de la violació de la seguretat de les dades personals, fins i tot, quan siga possible, les categories i el nombre aproximat d'interessats afectats, i les categories i el nombre aproximat de registres de dades personals afectades.

b) Nom i les dades de contacte del delegat de Protecció de Dades o d'un altre punt de contacte en el qual puga obtindre's més informació.

c) Descripció de les possibles conseqüències de la violació de la seguretat de les dades personals.

d) Descripció de les mesures adoptades o proposades pel responsable del tractament per a posar remei a la violació de la seguretat de les dades personals, incloent-hi, si escau, les mesures adoptades per a mitigar els possibles efectes negatius.

N/SEG/USU-007 USOS INDEGUTS DELS SISTEMES D'INFORMACIÓ

Amb caràcter general, es considerarà ús indegut dels sistemes d'informació en l'àmbit de la Diputació de València qualsevol conducta contrària al que es disposa en la present normativa per part dels obligats al seu compliment. No obstant això, s'enumeren seguidament un conjunt d'accions que es consideraran específicament un ús indegut dels sistemes d'informació de la Diputació de València.

N/SEG/USU-007-1 ÚS ABUSIU DE L'ACCÉS A INTERNET

Serà considerat ús abusiu de l'accés a Internet:

• L'accés a altres xarxes amb el propòsit de violar la seua integritat o seguretat.

• L'accés a continguts no relacionats amb les comeses professionals de l'usuari excedint un temps raonable, que interferisca en el rendiment professional o en l'eficiència dels recursos informàtics corporatius.

• Utilitzar l'accés a Internet per a l'ús de missatgeria instantània (WhatsApp, Messenger, Facebook Messenger, Skype, Line, Discord, Google Chat, Telegram, ShazzleChat, etc.).

• La transferència de fitxers no relativa a les activitats professionals de l'usuari (com ara jocs, fitxers de so, fotos, vídeos o pel·lícules, etc.).

• L'accés a recursos i pàgines web, o la descàrrega de programes o continguts que vulneren la legislació en matèria de Propietat Intel·lectual.

• La descàrrega de programes informàtics o fitxers amb contingut nociu que suposen una font de riscos per a l'organització.

• L'accés a Internet per a realitzar qualsevol activitat de promoció d'interessos personals.

• La publicació o l'enviament de missatges a través d'Internet que continguen amenaces, ofenses o imputació de fets que puguen lesionar la dignitat personal

i, en general, la utilització del servei d'Internet de manera il·legal o infringint aquesta o qualsevol altra norma interna que poguera resultar d'aplicació.

N/SEG/USU-007-2 ÚS ABUSIU DEL CORREU ELECTRÒNIC

Serà considerat ús abusiu del correu electrònic corporatiu:

• Utilitzar el correu electrònic corporatiu per a fins diferents als derivats de les activitats professionals.

• La utilització del correu corporatiu per a recollir correu de bústies que no pertanguen a l'organització, o la reexpedició automàtica del correu corporatiu a bústies alienes a l'organització.

• Usar qualsevol compte del correu corporatiu per a enviar missatges que continguen amenaces, ofenses o imputació de fets que puguen lesionar la dignitat personal i, en general, la utilització del correu electrònic de manera il·legal o infringint aquesta o qualsevol altra norma interna que poguera resultar d'aplicació.

N/SEG/USU-007-3 ÚS ABUSIU D'ALTRES SERVEIS I SISTEMES

Serà considerat també ús abusiu:

• L'accés a serveis i/o continguts dels sistemes d'informació amb el propòsit de violar la seua integritat o seguretat.

• L'execució de programes informàtics en els sistemes d'informació de la corporació sense la llicència d'ús corresponent.

• La reproducció, modificació, cessió, transformació o comunicació dels programes informàtics propietat de la corporació, llevat que els termes del llicenciament ho permeten i es compte amb l'autorització prèvia.

• L'ús, reproducció, cessió, transformació o comunicació pública de qualsevol altra mena d'obra protegida per drets de Propietat Intel·lectual, sense la deguda autorització.

• La transmissió, distribució o emmagatzematge de qualsevol material obscé, difamatori, amenaçador o que constituïsca un atemptat contra la dignitat de les persones.

N/SEG/USU-008 MONITORATGE I APLICACIÓ DE LA PRESENT NORMATIVA

La Diputació de València, per motius legals, de seguretat i de qualitat del servei, i complint en tot moment els requisits que a aquest efecte estableix la legislació vigent:

a) Revisarà periòdicament l'estat dels equips, el programari instal·lat, els dispositius i les xarxes de comunicacions de la seua responsabilitat.

b) Monitorarà els accessos a la informació continguda en els seus sistemes.

c) Auditarà la seguretat de les credencials i aplicacions.

d) Monitorarà els serveis d'Internet, correu electrònic i altres eines de col·laboració.

La Diputació de València durà a terme aquesta activitat de monitoratge sense utilitzar sistemes o programes que pogueren atemptar contra els drets constitucionals dels usuaris, com ara el dret a la intimitat personal i al secret de les comunicacions, i en tot moment es mantindrà la privacitat de la informació manejada, llevat que, per requeriment legal i investigació sobre un ús il·legítim o il·legal, siga necessari l'accés a aquesta informació, salvaguardant en tot moment els drets fonamentals dels usuaris.

Els sistemes en què es detecte un ús inadequat o en els quals no es complisquen els requisits mínims de seguretat, podran ser bloquejats o suspesos temporalment. El servei es restablirà quan la causa de la seua inseguretat o degradació desaparega.

El responsable de Seguretat dels Sistemes d'Informació i el Departament de Protecció de Dades i Seguretat de la Informació, cadascun en el marc de les seues competències, amb la col·laboració de la resta de les unitats de la Diputació de València, vetlaran pel compliment de la present normativa general i informaran el Comité de Seguretat TIC sobre els incompliments o les deficiències de seguretat observats, a fi que es prenguen les mesures oportunes.

El sistema que proporciona el servei de correu electrònic podrà, de manera automatitzada, rebutjar, bloquejar o eliminar part del contingut dels missatges enviats o rebuts en els quals es detecte algun problema de seguretat o d'incompliment de la present normativa. Es podrà inserir contingut addicional en els missatges enviats a fi d'advertir els receptors d'aquests dels requisits legals i de seguretat que hauran de complir en relació amb aquests correus.

El sistema que proporciona el servei de navegació podrà comptar amb filtres d'accés que bloquegen l'accés a pàgines web amb continguts inadequats, programes lúdics de descàrrega massiva o pàgines potencialment insegures o que continguen virus o codi nociu, conforme als criteris establits per a això pel Comité de Seguretat TIC. Igualment, el sistema podrà registrar i deixar traça de les pàgines a les quals s'ha accedit, així com del temps d'accés, el volum i la grandària dels arxius descarregats. El sistema permetrà l'establiment de controls que possibiliten detectar i notificar al responsable de Seguretat dels Sistemes d'Informació sobre usos prolongats i indeguts del servei.

Els **registres d'activitat** que puguen ser utilitzats com a prova en un procediment sancionador administratiu o en un procés judicial gaudiran de les garanties tecnològiques que asseguren que no poden ser alterats. Aquests registres **es trobaran sota la custòdia directa del responsable de Seguretat dels Sistemes d'Informació**, que serà l'únic que tinga permisos d'accés a la totalitat dels seus continguts, sense perjudici de les atribucions i competències del Departament de Protecció de Dades i Seguretat de la Informació i, si s'escau, del delegat de Protecció de Dades.

N/SEG/USU-009 COMPETÈNCIES I RESPONSABILITATS EN SEGURETAT DE LA INFORMACIÓ

Conforme estableix l'article 29 del Reglament pel qual es regula la política de seguretat i de la protecció de dades de caràcter personal en la Diputació de

València, i sense perjudici del que s'estableix en la norma en relació amb les mesures de seguretat de les dades de caràcter personal, el **responsable de Seguretat dels Sistemes d'Informació** és qui determina les decisions per a satisfer els requisits de seguretat de la informació i dels serveis, supervisa la implantació de les mesures necessàries per a garantir que se satisfan els requisits i reporta sobre aquestes qüestions.

En concret, **al responsable de Seguretat dels Sistemes d'Informació li correspon:**

• Actuar com a secretari del Comité de Seguretat TIC.

• Convocar el Comité de Seguretat TIC, i recopilar la informació pertinent.

• Ser responsable d'estar al corrent, juntament amb els diferents responsables de seguretat delegats, si s'escau, de canvis normatius (lleis, reglaments o pràctiques sectorials) que puguen afectar directament o indirectament la seguretat dels sistemes d'informació de la corporació, haver-se d'informar de les conseqüències per a les activitats de l'organització, alertar el Comité de Seguretat TIC, i proposar les accions oportunes d'adequació al nou marc normatiu.

• Elaborar i signar les declaracions d'aplicabilitat pertinents dels sistemes d'informació.

• Ser el responsable de la presa de decisions dia a dia entre les reunions del Comité de Seguretat TIC. Aquestes decisions estaran presidides pels principis d'unitat d'acció i coordinació d'actuacions en general i, especialment, en cas d'incidències que tinguen repercussió fora de l'organització i en cas de desastres.

• En cas de desastre s'incorporarà al Grup de Resposta a Incidents TIC i coordinarà totes les actuacions relacionades amb qualsevol aspecte de la seguretat dels sistemes d'informació.

• Coordinar les seues actuacions amb el Departament de Protecció de Dades i Seguretat de la Informació i col·laborar amb aquest en tots aquells aspectes que puguen incidir en les competències atribuïdes a aquest Departament.

Per la seua banda, l'article 32 del reglament citat estableix que el **Comité de Seguretat TIC** és l'òrgan que gestiona i coordina la seguretat dels sistemes d'informació TIC a nivell d'organització. Específicament li correspon:

• Coordinar totes les funcions de seguretat dels sistemes d'informació TIC de la Corporació.

• Vetlar pel compliment de la legislació i normativa interna d'aplicació.

• Recaptar del responsable de Seguretat informes regulars de l'estat de la seguretat de l'organització i dels possibles incidents. Aquests informes es consoliden i resumeixen per a la Direcció de la Corporació.

• Atendre les peticions d'informació que puga requerir el Departament de Protecció de Dades i Seguretat de la Informació, com també les recomanacions i propostes efectuades per aquest Departament.

• Coordinar i donar resposta a les inquietuds transmeses a través del responsable de Seguretat.

• Dinamitzar la disponibilitat de recursos per a atendre les necessitats de seguretat dels diferents sistemes d'informació, promoure inversions de caràcter horitzontal.

• Designar els components del Grup RITIC, indicat en l'article 15 de la present disposició.

El Comité podrà recaptar del personal tècnic propi o extern la informació pertinent per a la presa de les seues decisions, i també reclamar la presència del personal esmentat en les seues sessions o la seua incorporació a les comissions delegades de treball que pogueren constituir-se.

Finalment, l'article 35 del reglament referit atribueix al **Departament de Protecció de Dades i Seguretat de la Informació** una sèrie de competències i responsabilitats. Específicament, en matèria de seguretat de la informació li correspon:

• Elaborar el Pla General Auditor de Protecció de Dades Personals i Seguretat de la Informació de la Diputació i dur a terme les actuacions auditores hi compreses que li corresponguen.

• Executar l'auditoria de la seguretat dels sistemes d'informació a la qual es refereix l'Esquema Nacional de Seguretat.

• Supervisar el compliment de la normativa legal i interna en matèria de seguretat de la informació.

• Dur a terme investigacions sobre fets i incidents de seguretat de la informació.

• Elaborar estudis, propostes de regulació, documents per a facilitar el compliment normatiu i evacuar consultes i informes en la matèria.

• La difusió de tota mena d'informació i l'organització d'activitats que fomenten el coneixement, el compliment normatiu i les bones pràctiques en matèria de seguretat de la informació, tant en l'entorn corporatiu com en la societat en general.

Tots els empleats de la corporació estan obligats a facilitar tota la informació que els siga requerida pel Departament de Protecció de Dades i Seguretat de la Informació, com també l'accés a locals, instal·lacions, equips, arxius, suports d'emmagatzematge, programes, processos i procediments.

N/SEG/USU-010 INFORMACIÓ, DIFUSIÓ I FORMACIÓ

En virtut del que es disposa en l'article 42 del Reglament de política de seguretat i de la protecció de dades de caràcter personal en la Diputació Provincial de València, la corporació ha de garantir la formació i conscienciació a tots els seus empleats públics en matèria de seguretat de la informació.

L'objectiu general d'aquestes accions és evitar que els empleats públics puguen incórrer en la conculcació dels preceptes establits per la normativa de seguretat de la informació.

A aquest efecte, i com a objectius específics, les actuacions aniran dirigides a:

• Informar el personal de la normativa legal i interna que regula la seguretat de la informació, els deures i les responsabilitats que imposa, i les conseqüències que pot comportar el seu incompliment.

• Formar el personal en els coneixements i les habilitats professionals necessaris per a l'aplicació correcta de les polítiques i els procediments interns en la matèria, com també en el maneig de les eines tècniques que l'organització implante per a la gestió i compliment.

• Mentalitzar el personal de la necessitat d'incorporar als processos habituals de treball les previsions en matèria de seguretat de la informació.

• Mantindre actualitzat el personal en els possibles canvis legislatius i/o de la normativa interna en matèria de seguretat de la informació.

N/SEG/USU-010-1 INFORMACIÓ I DIFUSIÓ

Haurà d'habilitar-se un espai en la intranet corporativa en el qual tots els empleats tinguen accés al conjunt de normatives internes relatives a la seguretat de la informació. En la mesura que siga possible, s'utilitzarà també aquest espai per a la inclusió de tots aquells recursos que la Diputació dispose per a facilitar

la gestió i el compliment en la matèria. El Departament de Protecció de Dades i Seguretat de la Informació serà el responsable de donar contingut i administrar l'espai citat.

Podran utilitzar-se qualssevol altres instruments o vies que el Departament de Protecció de Dades i Seguretat de la Informació estime oportuns per a aconseguir l'objectiu d'informació per a aquells col·lectius o centres que, en atenció a les seues circumstàncies especials, no tinguen assegurat l'accés a l'espai en la intranet descrit anteriorment.

Amb independència del que es preveu en els paràgrafs anteriors, el personal directiu al capdavant dels diferents departaments i unitats haurà de procedir a donar la major difusió possible a les normatives i els recursos esmentats entre el personal del seu àmbit de direcció.

El Servei de Recursos Humans procedirà a incloure en els documents relatius a les noves incorporacions i renovacions de personal una referència a les obligacions i responsabilitats que s'adquireixen en matèria de seguretat de la informació.

N/SEG/USU-010-2 ACTIVITATS FORMATIVES

Les activitats formatives es duran a terme de conformitat amb allò disposat en l'article 42 del Reglament de política de seguretat i de la protecció de dades de caràcter personal en la Diputació Provincial de València.

El personal directiu al capdavant dels diferents departaments i unitats organitzarà degudament els seus recursos humans perquè el seu personal dependent perfeccione les accions formatives corresponents.

N/SEG/USU-011 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 foren 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.

En el cas que un usuari no observe algun dels preceptes assenyalats en la present normativa, sense perjudici de les accions disciplinàries i administratives que procedisquen i, si escau, les responsabilitats legals corresponents, es podrà acordar la suspensió temporal o definitiva de l'ús dels recursos informàtics assignats a aquest usuari.