

Consells de seguretat per a obres en construcció/ empreses i tallers amb vehicles tipus grues o amb plataforma

Vehicles i/ o maquinària

- Tanqueu els vehicles i no deixeu les claus a la mateixa nau
- Al final de la jornada tanqueu els accessos principals i perimetrals amb tots els sistemes de seguretat que disposeu
- A l'hora de deixar els vehicles i/o maquinària dins l'obra, escolliu sempre llocs fora de la vista de persones alienes
- Si detecteu individus que vigilen o circulen per la zona de forma repetitiva, retingueu les seves característiques (trets físics, vestimenta, plaques de matrícula...) i aviseu a la policia trucant al 112
- Instal·leu, si es possible, sistemes de localització dels vehicles
- Si es produís el robatori d'un vehicle o maquinària, és important posar-ho en coneixement de la policia el més aviat possible. Una resposta ràpida incrementa les possibilitats de recuperar el vehicle

Casetes d'obra

- Si disposa de finestres, eviteu que es puguin veure eines, materials o maquinària de valor
- No deixeu eines al costat de la caseta que podrien utilitzar-se per esbotzar els accessos
- Eviteu deixar les claus posades al pany de la caseta
- Assegureu-vos que el sistema de tancament de la caseta sigui de difícil obertura. En el cas de fer servir cadenats cal que siguin robustos
- No deixar a les casetes objectes personals (motxilles, carteres, telèfons mòbils...)

Davant de qualsevol dubte o aportació d'informació, podeu contactar amb la Policia de la Generalitat-Mossos d'Esquadra a través del telèfon 112.

Les comissaries estan obertes les 24 hores.

Gràcies per la col·laboració

Novembre. 2020

mossos d'esquadra



Recomanacions policials per als sistemes de videovigilància



**Generalitat
de Catalunya**



1 INTRODUCCIÓ

La finalitat d'aquest document és traslladar unes recomanacions policials per augmentar l'eficàcia dels sistemes de videovigilància (SVV) pel que fa a l'enregistrament de persones.

Aquestes recomanacions s'adrecen tant als emplaçaments que ja disposen d'un SVV com a aquells que pretenen instal·lar-ne un. Recull les indicacions policials per a la **instal·lació**, la **configuració**, l'**extracció d'imatges** i el **manteniment**. Finalment detalla com s'ha de realitzar l'**avaluació del sistema** un cop està en funcionament.

Els SVV són un eina imprescindible en la investigació policial, sobretot quan permeten la identificació de persones que participen en fets delictius. Gran part de la seguretat dels emplaçaments que disposen de SVV dependrà de la seva contribució a la tasca policial d'aquells enregistraments dels autors de fets delictius.

El primer pas per planificar la instal·lació o readequació d'un SVV és definir les seves necessitats així com el seu **objectiu** (fig.1). Per fer-ho, cal respondre a la pregunta: **Què es vol veure a les imatges i amb quina finalitat?** És molt diferent el que es voldrà veure en un sistema destinat a l'observació en una gran superfície comercial, que a la identificació dels usuaris d'una entitat bancària.

Els objectius dels SVV en l'àmbit policial es poden classificar en:

Observació: permet a l'observador que visiona les imatges determinar les característiques generals d'una persona, com per exemple la roba que vesteix o, de forma genèrica, l'activitat que duu a terme. La resolució o densitat de píxels aproximada de les imatges destinades a l'observació es situa en 100 píxels/metre (cada metre del camp de visió ha d'estar representat per 100 píxels).

Reconeixement: permet a l'observador que visiona les imatges determinar si la persona observada és una persona coneguda. La resolució o densitat de píxels aproximada de les imatges destinades al reconeixement es situa en 250 píxels/metre (cada metre del camp de visió ha d'estar representat per 250 píxels).

Identificació: permet a l'observador que visiona les imatges determinar les característiques físiques de la persona més enllà de tot dubte raonable. La resolució o densitat de píxels aproximada de les imatges destinades al reconeixement es situa en 500 píxels/metre (cada metre del camp de visió ha d'estar representat per 500 píxels).



Figura 1. Objectius dels SVV i resolucions mínimes d'imatge per a cada objectiu. En un mateix sistema, la posició de la persona determinarà l'objectiu que podrà assolir.

L'objectiu que pot assolir un SVV presenta una relació directa amb l'eficàcia pel que fa la capacitat d'identificar persones. Un sistema destinat a la identificació és més eficaç que un sistema destinat a l'observació. Per conèixer si el SVV assoleix l'objectiu pretès, i per tant quin es el seu nivell d'eficàcia, cal dur a terme la seva avaluació. En el punt 6 d'aquest document s'explica com dur a terme l'avaluació del sistema.

2 INSTAL·LACIÓ

Les recomanacions sobre la instal·lació fan referència a la **selecció**, l'**emplaçament** i la **protecció** de tots els elements que configuren el SVV.

2.1 Selecció dels equips

Han de presentar les característiques tècniques en base a la finalitat buscada, sobretot pel que fa al seu **nombre de píxels**.

El nivell d'**il·luminació** en les zones de pas obligat ha de ser adequat i suficient per observar amb claredat el rostre de les persones en totes les franges horàries. Cal utilitzar fonts de llum difusa amb l'espectre òptim per als equips de captació. Així mateix s'ha d'aportar il·luminació addicional per a aquelles zones d'escassa lluminositat, i optar per càmeres infraroges per a entorns amb baixa o nul·la il·luminació.

2.2 Emplaçament dels equips

S'ha de planificar la instal·lació del SVV en funció de l'objectiu perseguit, així com valorar la de les càmeres a instal·lar .

De forma genèrica, han d'estar situades en llocs que donin màxima cobertura a l'espai que es vol vigilar. Però també s'han d'instal·lar d'altres càmeres orientades a la identificació de persones.

Cal adequar la il·luminació de l'espai i la selecció de les característiques tècniques de les càmeres en funció dels factors ambientals. També cal eliminar els obstacles (panells informatius, cartells publicitaris, adhesius en vidres, etc.) que es troben en el camp de visió de les videocàmeres.

Les càmeres orientades a la **IDENTIFICACIÓ** de persones han de situar-se en zones de pas obligat. Aquestes zones són aquells punts on les persones han de passar obligatòriament per accedir, sortir o deambular per una instal·lació. També es poden ubicar d'altres càmeres en zones on es requereixi fer algun tipus d'operativa, com per exemple el pagament en comerços.

L'orientació de les càmeres ha de ser frontal al rostre de les persones que recorrin per aquests punts. L'altura d'instal·lació ha de ser la del rostre de les persones, aproximadament a 1,70 m sobre rasant (fig.2). En el cas que no sigui possible ubicar-la en aquesta altura, l'altura d'instal·lació no ha de superar un angle de 15 graus entre l'eix de visió de la càmera i el plànol horitzontal situat a l'alçada de la vista de les persones. Les càmeres zenitals es consideren totalment inapropiades per a la identificació de persones.



Figura 2. Valors recomanats d'alçada màxima de les càmeres orientades a la identificació de persones.

Exemple: Per una distància entre càmera i zona obligada de pas de 3 m, la càmera de seguretat hauria d'estar ubicada a una altura màxima de 2,4 m.



2.3 Protecció dels equips

S'ha de garantir la **protecció de les videocàmeres** contra factors climàtics, ambientals (pols, contaminació, etc.) i possibles actes vandàlics.

Les imatges s'han d'emmagatzemar en un **entorn segur** de forma que només hi pugui accedir el personal autoritzat, i no puguin ser manipulades ni sostretes. Es recomana assegurar físicament i lògicament (amb contrasenya) l'accés a les imatges enregistrades.

La captació i/o gravació d'imatges constitueix un tractament de dades personals sotmès a la normativa de protecció de dades regulat per la Llei Orgànica de Protecció de Dades¹.

Cal valorar la utilització de **sistemes d'alimentació ininterrompuda** (SAI) davant de possibles talls de subministrament elèctric.

1. Llei orgànica 3/2018, de 5 de desembre de protecció de dades personals i garantia de drets digitals.

3 CONFIGURACIÓ DEL SISTEMA

La configuració dels equips fa referència a la selecció de tots aquells paràmetres que afecten la captació i emmagatzematge de les imatges, tant de les càmeres com dels videogravadors. Es aconsellable adaptar la configuració a les característiques de l'emplaçament, ja que la configuració de fàbrica o els modes automàtics no sempre responen adequadament a les necessitats.

3.1 Resolució

La resolució és la capacitat d'un sistema per mostrar el detall de l'escena i s'expressa en nombre de píxels per unitat de distància. La resolució és el factor més determinant dels SVV per assolir l'objectiu perseguit (fig.3), ja que si el sistema no aporta un nivell de detall determinat de les persones que hi apareixen, aquestes no podran ser **observades**, **reconegudes** o **identificades**.

El equip orientats a la **IDENTIFICACIÓ** de persones han de presentar una resolució a partir de 500 píxels/metre o, el que és el mateix, de 80 píxels/rostre.



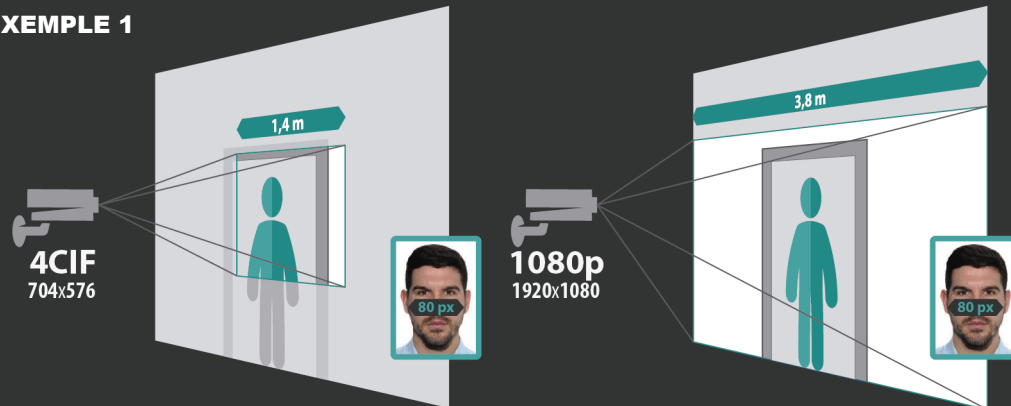
Figura 3. Imatges del rostre d'una persona mostrades a diferents resolucions. Per identificar una persona és necessària una resolució mínima de 500 px/m.

És important conèixer l'emplaçament on s'han de situar les càmeres de videovigilància, i per tant conèixer l'espai que han de cobrir. L'espai a cobrir (amplada de camp visual), la resolució del sistema i el seu objectiu són tres elements directament relacionats. Segons l'espai on s'ha de donar cobertura, l'objectiu que podem assolir vindrà donat per la resolució del nostre equip, es a dir, com més gran sigui l'espai on s'ha de donar cobertura, més gran haurà de ser la resolució del sistema per aconseguir el mateix objectiu (fig.4).

CAMP VISUAL MÀXIM QUE ES POT COBRIR SEGONS EL FORMAT I L'OBJECTIU BUSCAT

FORMAT	4CIF	720p	1080p	3Mpx	5Mpx	4K
OBSERVACIÓ	7,0 m	12,8 m	19,2 m	20,5 m	26,9 m	38,4 m
RECONeixEMENT	2,8 m	5,1 m	7,7 m	8,2 m	10,8 m	15,4 m
IDENTIFICACIÓ	1,4 m	2,6 m	3,8 m	4,1 m	5,4 m	7,7 m

EXEMPLE 1



EXEMPLE 2

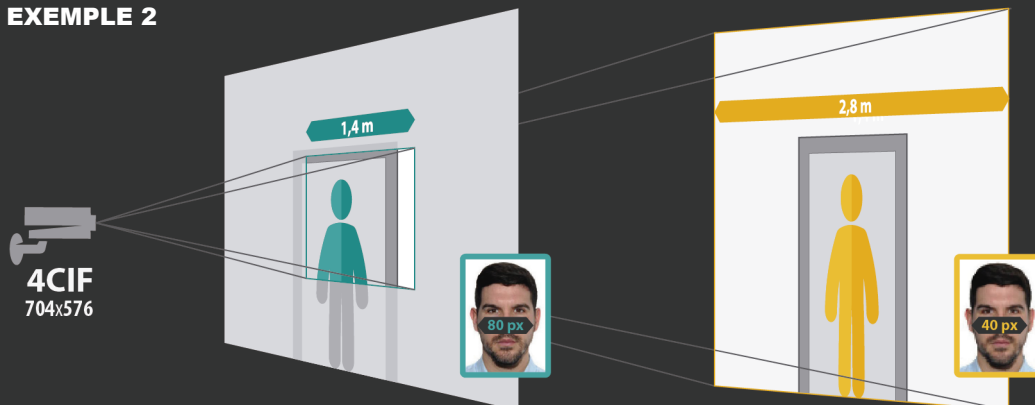


Figura 4. Valors de l'amplada del camp de visual per l'objectiu que es vol aconseguir, segons la resolució dels equips de captura.

Exemple 1: Si es vol **IDENTIFICAR** a les persones que accedeixen a un establiment per una zona de pas d'una amplada de 3,8 metres, serà necessari utilitzar un equip amb un format 1080p (1920x1080 px), mentre que si es vol obtenir el mateix objectiu, però amb un format de captura de 4CIF (704x576 px), el camp màxim visual que haurà de cobrir serà de 1,4 metres.

Exemple 2: Si es disposa d'un equip amb format 4CIF (704x576 px), i l'objectiu és **RECONÈIXER**, l'amplada del camp de visual haurà de ser de 2,8 metres. I si l'objectiu ha de ser **IDENTIFICAR**, l'amplada del camp de visió haurà de ser de 1,4 metres

3.2 Exposició

El **temps d'exposició** és el temps de captura de cada fotograma que compon una seqüència de vídeo. És molt important ajustar el temps d'exposició (*shutter*) per evitar que es produeixi el desenfocament per moviment. Per poder congelar el moviment d'una persona dins d'una imatge, i que aquesta es pugui observar de forma nítida, és necessari seleccionar un temps d'exposició adequat, en cas contrari, aquesta sortirà borrosa. Per a l'enregistrament de persones (velocitat deambulatoria habitual) es recomana seleccionar un temps d'exposició superior a d'1/200 segons.

La **sensibilitat lumínica** s'ha d'ajustar tant per minimitzar les alteracions que es produeixen en les imatges en condicions d'escassa il·luminació com per evitar els contrallums en condicions d'excés d'il·luminació. Molts equips permeten configurar el nivell de sensibilitat lumínica, l'amplitud de rang lumínic i la compensació de diferents fonts de llum.

3.3 Taxa de fotogrames (FPS)

S'ha de seleccionar un nombre de fotogrames per segon que permeti seguir i ubicar l'objectiu de l'enregistrament dins de l'espai sota vigilància. En les càmeres destinades a la identificació, cal utilitzar una taxa mínima de 6 fotogrames per segon (fps).

3.4 Compressió

La compressió de les imatges s'ha de realitzar sense comprometre'n la qualitat. Elevats nivells de compressió sovint comporten baixos nivells de qualitat de les imatges i la creació d'artefactes. La correcta relació entre qualitat d'imatge i compressió sempre s'ha d'establir utilitzant imatges de subjectes en moviment, ja que és sobre aquests on els efectes de la compressió són més adversos.

3.5 Data i hora

El sistema ha de tenir actualitzades la data i l'hora. Localitzar un esdeveniment concret, dins una seqüència de vídeo, en un equip mal configurat produirà un cost afegit innecessari. Cal evitar que aquestes dades, com d'altres que es puguin mostrar en pantalla, ocultin el camp de visió. És molt recomanable que el programari d'exportació permeti ocultar les dades en el cas que sigui necessari.



3.6 Conservació dels enregistraments / Període de sobreescritura

S'han de conservar els enregistraments el termini marcat per la normativa vigent. Per complir amb la normativa, s'ha d'evitar sempre la reducció de la resolució, de la taxa de fotogrames o l'augment de compressió dels fotogrames.

Quan s'enregistri un fet delictiu o infracció administrativa, s'han de conservar les imatges amb l'única finalitat de posar-les a disposició de l'autoritat competent sense que es puguin utilitzar per cap altre propòsit.

3.7 Detecció de moviment

Es recomana l'enregistrament continu, i desactivar l'opció d'enregistrament per moviment, especialment en zones sensibles o amb un elevat trànsit. D'aquesta forma s'evitarà que l'enregistrament per moviment pugui quedar interromput durant esdeveniments importants.

4 EXTRACCIÓ DE LES IMATGES

El sistema ha de permetre l'extracció de les imatges a un suport extraïble (llapis de memòria, disc dur, CD, etc.) en un format sense pèrdua de qualitat. En cas que no sigui possible, l'alternativa serà el lliurament de l'aparell videogravador.

Les imatges han de ser lliurades a les forces i cossos de seguretat en un format estàndard d'arxius, en cas contrari, cal aportar el programari propietari de reproducció. Aquest programari ha de permetre les següents operacions: capturar el fotograma seleccionat, reproduir endavant/enrere, seleccionar velocitat de reproducció, reproduir fotograma a fotograma, mostrar/ocultar les metadades (càmera, data, hora, propietats de l'arxiu) i visualitzar a màxima resolució una o diverses càmeres.

Els arxius d'imatge exportats han d'incloure les metadades de l'enregistrament: data, hora, dimensions en píxels, còdec utilitzat, i la identificació de la càmera en cas que existeixi més d'una.

5 MANTENIMENT

Es recomana planificar un calendari d'inspeccions periòdiques de manteniment del sistema. Aquest manteniment ha d'incloure la revisió dels elements relacionats amb la instal·lació (orientació, il·luminació, protecció, obstacles en la visió, SAI, etc.), la revisió de la configuració del sistema (resolució, exposició, fps, compressió, data i hora, canvis de contrasenya, etc.) i la neteja d'equips i carcasses protectores. Cal valorar la substitució dels elements que presentin defectes no reparables.

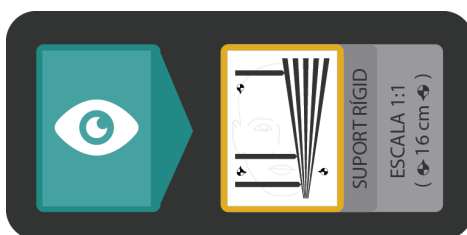
6 AVALUACIÓ

L'avaluació del SVV ha de permetre conèixer si el sistema podrà assolir l'objectiu pretès.

Passos a seguir:

1. Imprimiu la plantilla d'avaluació annexa al document, enganxeu-la sobre un suport rígid o plastifiqueu-la.

ATENCIÓ: comproveu que està a escala 1:1, mesurant amb un regle i verificant que entre els punts de registre (⊕) hi ha 16 cm. (a les preferències d'impressió, el document ha d'estar ajustat a la mida real).

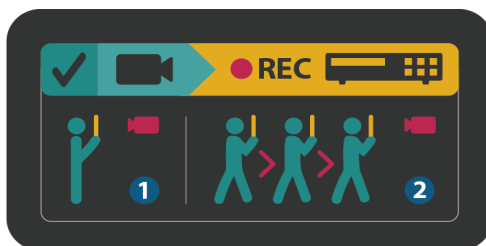


2. Escolliu la càmera que voleu avaluar.

3. Realitzeu dos enregistraments:

Primer enregistrament. Situeu-vos al punt on es vol avaluar el sistema (Exemple: sota el marc de la porta d'accés dels clients a l'establiment). Subjecteu la plantilla davant del rostre, de forma perpendicular al terra, durant uns segons, mentre el sistema fa l'enregistrament.

Segon enregistrament. Camineu, amb la plantilla davant del rostre travessant el punt on es vol avaluar el sistema.

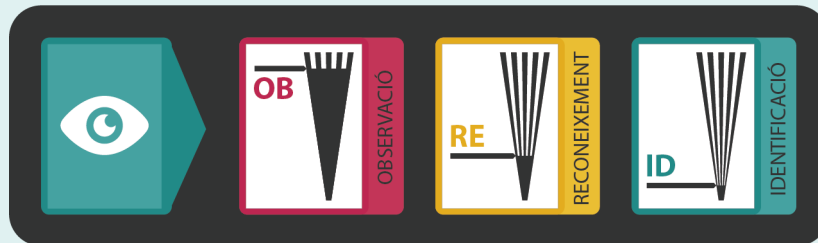


4. Feu l'extracció dels fotogrames dels dos enregistraments a la màxima qualitat disponible, màxima mida disponible i format sense pèrdua (TIF, BMP, PNG...).





5. Comproveu el nivell màxim de detall que es pot arribar a observar a la plantilla d'avaluació dels fotogrames extrets. Determineu fins a quin punt es poden discriminar de forma independent les cinc línies (franges negres i blanques). **Aquest serà l'objectiu que podrà assolir el vostre sistema.**



Els equips orientats a la **IDENTIFICACIÓ** de persones haurien de poder discriminar les franges de **2mm de gruix**.

IMPORTANT

L'avaluació sempre s'ha de realitzar sobre els fotogrames extrets de l'enregistrament del videogravador i no sobre les imatges que es visualitzen en directe sobre el monitor.

La visualització en directe sobre pantalla us mostra les imatges segons la resolució de la vostra pantalla i això pot alterar la resolució real dels fotogrames enregistrats pel vostre sistema.

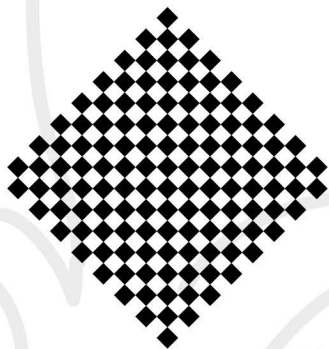
PLANTILLA D'AVALUACIÓ

OBSERVACIÓ (100 px / m)



INSTRUCCIONS: IMPRESSIÓ ESCALA 1:1

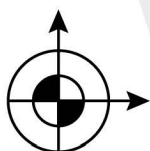
Un cop impresa la plantilla, confirmar que la distància entre els punts de registre (●) és de 16 cm.



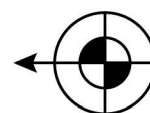
IDENTIFICACIÓ

2x2 mm

RECONeixEMENT (250 px / m)



IDENTIFICACIÓ (500 px / m)



mossos d'esquadra





Recomanacions policials per als sistemes de videovigilància

**L'adopció de totes aquestes recomanacions
dels sistemes de videovigilància ajudarà a:**

- Dissuadir la comissió de fets delictius
- Augmentar la identificació de persones que participen en la comissió de fets delictius
- Disminuir la intervenció policial en l'activitat dels establiments que disposen de SVV
- Garantir l'eficàcia dels sistemes de videovigilància

mossos d'esquadra



**Generalitat
de Catalunya**



Prevenció

Frau i riscos Internet



Mesures de prevenció generals

- 🔒 **Tenir contrasenyes segures/robustes, que no es puguin deduir. Tot seguit es detalla les característiques d'una contrasenya segura.**

Una contrasenya segura ha de tenir al menys tres d'aquestes quatre característiques:

- 🔒 Tenir números
- 🔒 Tenir lletres
- 🔒 Tenir majúscules i minúscules
- 🔒 Tenir símbols (!, \$, %, &, #, etc.)

També ha de complir els següents requisits:

- 🔒 Longitud no inferior a vuit caràcters
- 🔒 No ha de formar-se amb números i lletres consecutius al teclat
- 🔒 No ha de contenir informació fàcil d'endevinar, com ara la informació personal
- 🔒 No ha de contenir paraules existents en cap idioma

I per últim, però igual d'important, s'ha de:

- 🔒 Tenir una contrasenya per a cada servei
- 🔒 S'ha de canviar amb certa freqüència
- 🔒 Guardar la contrasenya en un lloc segur i no donar-la a ningú

- 🔒 **Utilitzar només connexions WIFI segures, evitar les gratuïtes, per exemple per fer operacions bancàries en xarxes gratuïtes tenen més probabilitats de ser objecte d'un frau que puguin aconseguir les claus d'accés (Phishing bancari). A més per poder fer ús de connexions gratuïtes ens poden demanar dades personals i contrasenyes de xarxes socials, amb aquesta informació es facilita l'entrada a la pàgina personal ja sigui d'una entitat bancària, xarxa social....**
- 🔒 **Desconnectar el Bluetooth quan no es necessita. Hi ha programes que escolten les trucades (Ex. Car Whisperer), d'altres poden tenir accés al telèfon de l'usuari i utilitzar les seves funcions (Ex. Bluebugging).**
- 🔒 **No identificar la WIFI o el Bluetooth amb el nom propi o altres dades personals que es podrien identificar fàcilment.**
- 🔒 **Tenir actualitzat el sistema operatiu, les APP, l'antivirus i utilitzar talla focs (el qual s'encarrega de vigilar els accessos entre l'ordinador i la xarxa. A més, bloqueja totes les connexions que no estan permeses explícitament.)**
- 🔒 **Xifrar/codificar els dispositius d'emmagatzematge extern. Es pot fer en qualsevol moment utilitzant un programari adequat.**
- 🔒 **Prestar atenció a la instal·lació de programaris en els PC, tablets o telèfons mòbils. Especialment en el que es detalla en els permisos.**
- 🔒 **No posar informació privada o que ens pugui comprometre en perfils oberts de xarxes socials.**



Mesures de prevenció per tipus de frau

Phishing bancari (o suplantació d'identitat)

En aquest tipus de frau es cerca aconseguir contrasenyes diverses (d'identificació d'usuari bancari, el n. de targetes de crèdit, el n. de compte) amb la finalitat de poder fer transaccions amb els diners de la víctima. *Exemples: correu electrònic que simula ser la nostra entitat bancària i que ens sol·licita canviar la contrasenya que disposem, ja que ha caducat.*

Prevenció

- 🔒 No obrir correus d'usuaris desconeguts o que no s'hagin sol·licitat. Fins i tot, eliminant-los directament sense obrir cap enllaç o arxiu adjunt.
- 🔒 Si es tracta de la web d'un banc, sempre vindrà detallada en l'adreça del navegador/URL de manera xifrada/segura i inclourà "s" https://, a més de figurar la imatge d'un cademat.
- 🔒 És important no accedir a serveis de banca on line a través d'ordinadors públics o xarxes WIFI.
- 🔒 Cal recordar que les entitats bancàries no demanen mai dades personals als seus clients per correu electrònic, ni tampoc targetes bancàries o de coordenades o dades d'usuari i contrasenya. Si es reben aquest tipus de sol·licituds per correu, no és el banc.

SMS Premium

Són números, normalment de cinc xifres, que estan regulats i són legals. Cerquen un parany perquè la víctima (enviï un SMS) faciliti el seu telèfon mòbil. Sovint es cau en el parany perquè pensem que només són publicitat sense saber que aquests missatges tenen un cost elevat.

Exemples:

- Subscripció voluntària o involuntària d'un usuari a una base de dades que li envia informació sobre certs temes (generalment jocs i concursos), però li cobren per cada SMS rebut.
- Per Facebook, t'etiqueten en un vídeo i si els vols veure et demanen el número de mòbil. Si el poses ja està subscrit a SMS Premium.
- Missatge Whatsapp on t'informen d'una aplicació gratuïta nova que pot ser del teu interès. Et demanen el número de mòbil i et subscriuen al SMS Premium.

Prevenció / com identificar número de SMS Premium

- 🔒 Trucar a la nostra operadora i sol·licitar que doni de baixa i bloquegin tots els serveis SMS Premium i els números de tarificació addicional
- 🔒 Es componen de 5 a 7 xifres i comencen per 25, 27, 28, 29, 35, 37, 39, 79 o 99.



Ransomwares

És un tipus de malware (programes maliciosos) que restringeix l'accés a determinades parts o arxius del sistema infectat, i demana un rescat a canvi de treure aquesta restricció. Es transmet tant com un *troià* com un *cuc* infectant el sistema operatiu. En aquest punt el ransomware s'iniciarà i xifrarà els arxius amb una clau que només coneix el creador. Aquest tipus de frau es pot rebre a través del correu electrònic o la consulta de determinats enllaços maliciosos a través d'Internet. *Exemple: Es rep un correu on consta com a remitent/assumpte "correos" amb el que s'informa que el destinatari ha de recollir un paquet o una carta. Dins el correu hi ha un enllaç que suposadament és per gestionar la recollida, el qual enllaça amb una pàgina web que suplanta la identitat de Correos y Telégrafos, on es sol·licita la introducció d'un codi per a consultar l'estat detallat de l'enviament. Si s'omple el codi i es prem "consultar" s'inicia la descàrrega d'un codi maliciós ransomware.*

Prevenció

- 🔒 No obrir el correu d'usuaris desconeguts o que no hagin estat sol·licitats.
- 🔒 Esborrar el correu sense obrir-lo i assegurar-nos també d'esborrar-lo definitivament de la carpeta dels elements suprimits o esborrats.
- 🔒 Revisar el contingut dels missatges que es rebem, i també els que enviem per evitar enviar-los a destinataris equivocats
- 🔒 Guardar la informació en mitjans d'emmagatzematge externs, per evitar perdre informació dels clients, facturació...
- 🔒 Apagar l'ordinador al més aviat possible, fins i tot desendollant el cable corrent. El xifrat d'arxius és un procés llarg, si aconseguim aturar-lo aviat, és possible que la majoria dels nostres documents estiguin intactes.
- 🔒 No intentar desinfectar la màquina immediatament, esborrant fitxers sospitosos o formatant la màquina. Es podrien perdre fitxers necessaris per trencar el xifrat dels nostres documents.

Altres modalitats de frau

o **Estafa en compres online**

A través de pàgines web que venen productes que no existeixen i que, tot i pagar, no es rebran. Per exemple vehicles d'alta gama.

o **Estafes de caritat**

Es suplanta una organització de caritat sol·licitant donacions para catàstrofes naturals, malalties o per atendre a una mare o fill malalts. Poden arribar a utilitzar-se logotips d'organitzacions prestigioses.

o **Oferta treball (des de casa/oportunitat de negoci)**

Aquest tipus d'estafes té molta varietat, i inclou des d'intents per aconseguir accés a la informació personal i privada de la persona que cerca feina (com ara comptes bancaris, números d'identificació personal, ...) fins a requeriments de pagar una taxa per a poder entrar dins la llista de candidats a aconseguir una possible feina.

o **Scam** (també anomenat frau 419, scam 419, o engany nigerià)

La denominació 4-1-9 ve del número de l'article del codi nigerià que sanciona aquest tipus de frau. Aquest frau es presenta generalment sota la forma d'una persona (en alguns casos es presenta com a familiar llunyà) que afirma posseir una important suma de diners (diversos milions de dòlars d'una herència, suborns, comptes sense hereu, fons a col·locar a l'estranger per un canvi de context polític, etc.) i demana l'ús d'un compte per transferir ràpidament aquests diners.

o **Virus policial**

En aquest cas apareix un missatge dient que estava mirant pornografia o fent descàrregues il·legals per la qual cosa ha de pagar una sanció de 100€.



Frau a Internet



Per denunciar



Per consultar

internetsegura@gencat.cat



112
emergències