Apunts tècnics per a la indústria

10

# Ciberseguretat bàsica

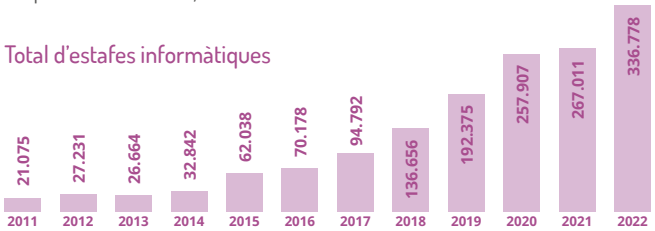
Manual d'ús per a sistemes d'informació i comunicació a l'empresa

Can Muntanyola
Centre de Serveis a les Empreses

# Per treballar es necessita tranquil·litat

Aconseguir tranquil·litat en l'àmbit del treball pot ser complicat. L'ús de la tecnologia creix perquè ens permet ser més eficients, però alhora augmenten els seus riscos. La ciberseguretat existeix perquè hi ha ciberdelinqüència, la qual avança en els seus mètodes: robatori de dades, usurpació de personalitat, entre d'altres fraus.

Els sistemes d'informació de l'empresa són cada cop més rellevants, perquè hi conflueixen les dades personals de moltes persones: informació financera, secrets i propietat industrial, traçabilitat i certificacions de productes, control de la producció i de la cadena de subministrament de les parts interessades, etc




Font: Secretaria d'estat de seguretat -Ministeri de l'interior

## FAQ . Qui està interessat a robar informació?

La ciberdelinqüència és una branca de la delinqüència que comet delictes al món digital.

La seva expansió i augment van directament relacionats amb l'increment d'importància dels actius que hi ha digitalitzats.

El robatori d'informació, de tot tipus, és lucratiu perquè hi ha tant la possibilitat de vendre-la a tercers com extorsionar les empreses afectades, fer xantatge a les persones afectades pel robatori de les seves dades, etc.

## La seguretat és cosa de tots

Els departaments TIC posen tots els mitjans tècnics disponibles (antivirus, tallafoc, antispam, etc.) per protegir els usos de les tecnologies de la informació i la comunicació (TIC). Però aquests mitjans poden ser insuficients degut a l'encara poca maduresa tecnològica de les mesures de ciberseguretat.

Actualment, per combatre els ciberriscos encara és necessària la col·laboració dels usuaris del sistema d'informació, ja que no disposem de tecnologia per autenticar els usuaris autoritzats, i són els empleats qui guarden les claus d'accés i qui amb les seves conductes poden ser les portes d'accés dels ciberdelinqüents. Per no caure en les trampes de la ciberdelinqüència, cal treballar sempre amb tranquil·litat i tenir un entorn i organització que ho faciliti.

L'empresa no pot cometre l'error de creure que la informació està segura gràcies a l'existència d'eines, programes i aparells que protegeixen. La ciberdelinqüència sempre busca oportunitats provocant les errades dels humans i, per tant, la seguretat és cosa de tots.

## L'empresa és la responsable de la ciberseguretat

Malgrat l'important rol dels empleats usuaris de les TIC en la ciberseguretat, les seves responsabilitats no es poden descarregar en ells ni es poden delegar en experts externs, perquè l'empresa és responsable de la ciberseguretat i és qui respon dels danys que un ciberatac pugui causar a tercers. I, per tant, ha d'impulsar un pla de ciberseguretat en tots els seus aspectes: organitzatiu, legal, formatiu, social, ètic i tecnològic.

Aquesta fitxa en Ciberseguretat recull les principals mesures i instruccions que han de formar part de les actuacions més bàsiques en ciberseguretat de qualsevol empresa.

# Els responsables de la ciberseguretat

L'empresa que vol treballar la ciberseguretat, com a primera mesura necessita un equip o una persona responsable de ciberseguretat que sigui el referent tecnològic de tot el personal, i marqui les conductes i instruccions a seguir pel que fa a ciberseguretat.

Si l'empresa no disposa d'un perfil intern capacitat per ser el responsable de ciberseguretat, convé que sigui extern. Les següents indicacions també us podran servir per saber què hem de demanar a una empresa externa que ens porti la ciberseguretat.

**Atenció!** Cal que, al responsable de ciberseguretat (intern o extern), que és qui té accés al control de totes les claus de l'empresa, li tinguem la màxima confiança i èticament sigui infal·lible a cap temptació de ciberdelinqüència.

Un responsable de la seguretat de la informació en una empresa té diverses funcions clau, recollides en l'article 7 de l'RD 43/2021 de seguretat de les xarxes i sistemes d'informació:

1. Establir i mantenir la política de seguretat de la informació de l'empresa (pla de ciberseguretat).
2. Supervisar i gestionar tots els riscos de seguretat de la informació, tant tecnològics com organitzatius.
3. Assegurar-se que l'empresa compleix totes les lleis i regulacions pertinents.
4. Coordinar les auditories de seguretat i investigar qualsevol incident de seguretat.
5. Proporcionar formació i conscienciació sobre seguretat de la informació a tot el personal.
6. Gestionar la resposta a incidents de seguretat i la recuperació després d'un incident.
7. Supervisar la implementació i el manteniment de controls de seguretat.

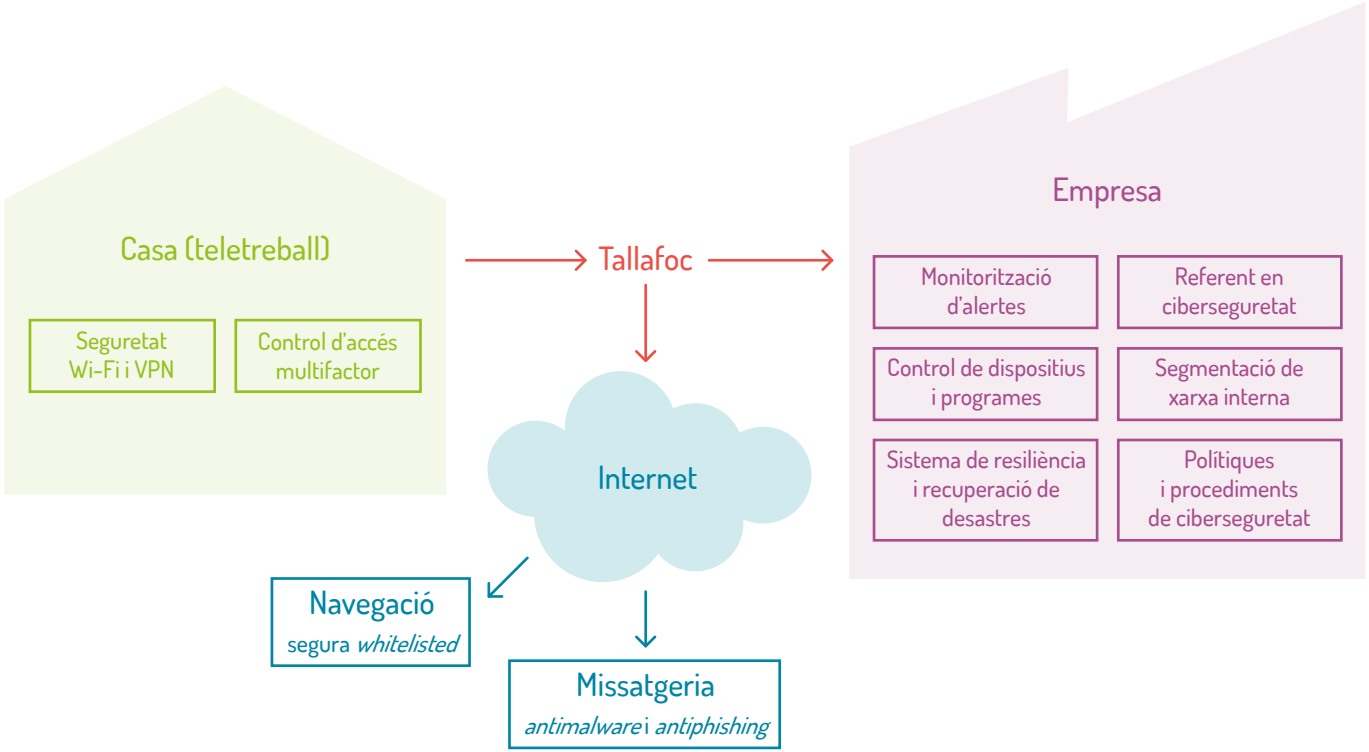
## FAQ . Perquè les TIC són insegures?

Totes les tecnologies són insegures. A més el nivell de seguretat d'una tècnica decreix quan augmenta la seva maduresa. Durant l'inici de les fàbriques tèxtils hi havia uns nivells d'inseguretat molt superiors als que hi ha avui en dia.

En l'àrea de les TIC som als inicis del seu ús i la nostra experiència i maduresa no permet assolir els nivells de seguretat que tothom desitjaria.

## Les mesures tecnològiques dels responsables de la ciberseguretat

Una de les tasques principals és estructurar les mesures físiques i de programari que ens poden ajudar a gestionar la ciberseguretat:



1. Incorporar tecnologies de monitorització, perfilat i registre que graven i informen de les accions que fan tots els instruments i els treballadors quan estan connectats, sigui tant a la xarxa de l'empresa com en accessos remots. Aquestes tecnologies la subministren programes de cibervigilància. Ens permetran prendre decisions informades en situacions de contingència quan es detecti una alerta de seguretat, analitzar quins forats hi ha en les polítiques de ciberseguretat i donar instruccions clares als nostres empleats.
2. Implantar còpies de seguretat dels programes per poder reprendre l'activitat i recuperar la informació en poques hores en casos de ciberatacs. Cal que es facin simulacres anualment per comprovar l'efectiva recuperació de les còpies en els temps acordats.
3. Implementació de programari antivirus: programari maliciós (*malware*), programari de segrest (*ransomware*), programari espia (*spyware*), filtres de pesca de credencials (*antiphising*) inundació (*antispam*) per al correu electrònic i programari de llista blanca (*whitelisting*), per prevenir les diferents maneres d'accedir a les nostres xarxes i programaris des del navegador.
4. Mantenir els programes i eines que utilitza l'empresa actualitzats (especialment els antivirus), per tenir al dia les errades i novetats de seguretat detectades pels propis proveïdors de programaris i eines digitals.
5. Segmentació de la xarxa interna i implantació de tallafocs (*fire-walls*) entre les diverses xarxes que utilitza l'empresa, tant internes com externes, perquè ens permet definir un conjunt de regles per permetre, denegar o bloquejar l'accés dins la xarxa. En les empreses industrials és especialment important aquesta segmentació per separar els programaris específics dels diferents departaments o divisions d'una empresa, amb la qual cosa s'evita que un possible atac o fallada en una part de la xarxa afecti la resta de l'organització, i més en aquelles indústries on hi ha processos crítics que no poden permetre cap interrupció. També la segmentació de la xarxa facilita la gestió i el manteniment dels actius més crítics. Al tenir-los aïllats en una xarxa separada, és més fàcil controlar i supervisar els dispositius i els recursos associats a aquests actius. Això permet una millor detecció i resolució de problemes, així com una millor planificació i implementació de les actualitzacions i les millores necessàries..
6. Implantació de programes generadors i gestors de contrasenyes corporatius, perquè els empleats usuaris de TIC puguin gestionar amb més seguretat els accessos als programes TIC, sense haver de memoritzar o apuntar contrasenyes.
7. Implantar programes de xifrat de dades i carpetes, en aquells programaris amb dades de valor, en les comunicacions amb tercers realment confidencials o estratègiques, o si emmagatzemem informació al núvol.

# Les funcions organitzatives del responsable de ciberseguretat

La persona responsable de ciberseguretat, com que la tecnologia de ciberseguretat no és prou madura, ha d'aconseguir una conscienciació transversal entre tots aquells que accedeixin a la informació i garantir la implicació del personal per col·laborar en la detecció i notificació d'incidents de ciberseguretat i seguiment de protocols de resposta. Per això, és necessari que l'empresa creï un entorn on tothom sigui conscient dels riscos, s'identifiqui com a vulnerable i desitgi millorar davant dels riscos innats a les TIC.

Les actituds de desconfiança i de prudència dels empleats usuaris de les TIC són bones companyes de la ciberseguretat.

## 1 Avaluar i informar els empleats

Tots els empleats han de complir uns compromisos bàsics que permetin mantenir un nivell de ciberrisc acceptable. S'ha de marcar els coneixements i conductes de ciberseguretat dins l'entorn de l'empresa i començar, per tant, per avaluar els coneixements de què parteix cada empleat i de la seva actitud davant la ciberseguretat i definir un pla de comunicació sobre instruccions i comportaments.

**Es pot utilitzar el qüestionari d'avaluació annex per fer l'avaluació.*

### Instrucció 1

És imprescindible que tots els empleats coneguin el canal de comunicació amb el responsable de ciberseguretat (telèfon i correu electrònic) per a la notificació d'incidències i/o per resoldre els dubtes que els puguin aparèixer.

### FAQ . Per què és necessari notificar una incidència en ciberseguretat?

Darrere d'una incidència de ciberseguretat sempre hi ha una informació que s'ha posat en risc. L'única manera de limitar l'impacte i/o l'abast del risc que s'ha patit és conèixer-lo.

## 2 Utilitzar només eines i aplicacions autoritzades

És primordial que el responsable de ciberseguretat eviti el descontrol de la informació i cal que informi al personal que només es poden utilitzar les eines i aplicacions autoritzades i monitoritzades per part de l'empresa. Encara que, com a usuaris d'Internet, coneguin programes o pàgines web que els permetin realitzar certes tasques, s'ha d'indicar que, com a empleats, no les utilitzin si no és amb el vistiplau del seu referent en ciberseguretat.

### Instrucció 2

Cal recordar a tots els empleats que molts delictes informàtics acostumen a falsificar identitats en missatges a persones treballadores per confondre'ls i robar-los informació, contrasenyes, etc., i explicar als empleats que només utilitzin els sistemes de missatgeria de l'empresa. Tota la resta de canals no són de confiança i deixen la persona usuària i la xarxa de l'empresa desprotegida.

### Instrucció 3

Així mateix, també cal formar els treballadors per verificar el nom de les adreces (les URL) a les quals es connecten a partir d'enllaços de missatges que reben. No és suficient que el disseny i la interfície de les webs a què porten els enllaços sigui la mateixa de sempre, perquè els ciberdelinqüents la poden replicar per generar un engany i estafar-te.

### Instrucció 4

L'empresa necessita implementar polítiques de mínim privilegi per assegurar que cada persona usuària només té accés a les eines i programaris per exercir les seves funcions.

## 3 Assegurar les claus i certificats digitals

Protegir les contrasenyes i fer-les verdaderament complexes, avui en dia, no ho poden fer les persones, com fins ara. Memoritzar les contrasenyes actualment té tants riscos que la robin com tenir-la apuntada. Aquestes credencials d'accés obren la porta al món digital de l'empresa i cal protegir-les amb noves mesures.

En certs casos, la teva identitat també pot basar-se en l'ús d'algun certificat digital. Aquests certificats permeten que una tercera entitat confirmi qui és l'usuari i cal tenir la mateixa cura que amb les contrasenyes, respecte a la seva custòdia.

### Instrucció 5

Si vols obtenir una bona (complexa) contrasenya, pots utilitzar generadors. Com per exemple: *https://www.lastpass.com/password-generator*. Si no utilitzes generadors, forma en la creació i custòdia de contrasenyes complexes seguint les instruccions que trobaràs al "Full de trucs".

### Instrucció 6

Perquè el personal no hagi de memoritzar contrasenyes i puguin ser enganyat en webs amb URL falses, implanta i obliga a fer ús d'un gestor de contrasenyes autoritzat per l'empresa, que permet emmagatzemar totes les contrasenyes de forma segura recordant només una clau mestre.

### Instrucció 7

Per millorar el control d'accés remot també has de configurar el segon factor d'autentificació. Així t'assegures que, malgrat t'encertin o et robin la contrasenya, també sigui necessari el teu mòbil, la teva targeta intel·ligent, clau USB, etc.

## 4 Protegir els dispositius

Tingues un inventari actualitzat dels dispositius de l'empresa i estableix un sistema de gestió centralitzat i protegeix els dispositius (ordinadors, telèfons, tauletes) que utilitzis per treballar.

Com que serà un dispositiu que tindrà accés a la informació confidencial de l'empresa, és important limitar-ne l'ús als usuaris autoritzats (instrucció 4). És important mantenir-lo actualitzat, tant el sistema operatiu i molt especialment les eines d'antivirus, i bloquejar el dispositiu tan aviat s'abandoni l'ús. No permetis que altres persones en facin ús.

### Instrucció 8

Cal nformar a tot el personal que cal que evitin utilitzar els dispositius de l'empresa altres membres de la família, amics, etc., per usos particulars, i supervisa'n l'ús. També cal prohibir connectar llapis de memòria compartits o desconeguts.

### Instrucció 9

Està expressament prohibit manipular els equips i programes sense el coneixement i l'autorització dels responsables de TIC i ciberseguretat.

L'empresa pot habilitar mecanismes per monitoritzar els dispositius, assegurar-ne la integritat i detectar intents malintencionats de manipulació.

En el cas dels telèfons mòbils s'ha d'assegurar que tinguin les memòries encriptades, les claus d'accés i un mecanisme de destrucció remota en cas de pèrdua. Totes aquestes mesures ofereixen tranquil·litat i confiança per posar-hi informació.

## 5 Protegir la Wi-Fi

La xarxa Wi-Fi de l'empresa ha de tenir una contrasenya complexa i robusta per prevenir un sabotatge extern.

Les regles per a una contrasenya segura també poden emprar-se per les de la Wi-Fi però allargant la longitud fins als 24 caràcters. Evita utilitzar la contrasenya predeterminada.

Es recomana emprar una connexió VPN sempre que sigui possible.

### Instrucció 10

Cal conscienciar i informar els treballadors d'evitar la utilització de xarxes Wi-Fi que no siguin de confiança. És a dir, evita xarxes públiques desconegudes.

## 6 Correu electrònic

El correu electrònic és l'eina bàsica oficial de comunicació propietat de l'empresa, i cal garantir-ne un ús correcte i evitar el màxim l'entrada de correu brossa. Com a propietaris, l'empresa pot accedir i revisar l'ús i contingut d'aquesta eina.

### Instrucció 11

Cal recordar a tots els seus usuaris que hem d'evitar l'ús de caire personal del correu corporatiu i restringir-ne l'ús a l'àmbit professional, i que el correu electrònic sol ser el principal mitjà d'entrada dels ciberdelinqüents.

### Instrucció 12

Cal recordar als empleats que davant de qualsevol dubte sobre un correu, no es respongui i s'enviï al responsable de ciberseguretat perquè l'analitzi i previngui la resta d'empleats si fos necessari.

Les formes més habituals de correu brossa són:

- **SPAM:** correu publicitari no desitjat. És important avisar el referent que aquest correu ha esquivat els filtres, però sobretot no respondre-hi, enviar confirmació de rebuda ni clicar cap enllaç o imatge que pugui dur.
- **PHISHING:** correu que pretén fer-se passar per algú altre per aconseguir privilegis o informació delicada en el mateix correu o a través d'un canal que ens suggereix. Cal avisar el referent i tenir molt present quins són els canals oficials perquè se'ns demani informació sensible i consultar la direcció a la mínima sospita.

## 7 Xarxes socials i missatgeria instantània

Aquests són nous canals de comunicació on el contingut que hi publiquem pot deixar rastre de la nostra activitat professional i podem perdre confidencialitat. Cal ser molt curós en el seu ús i restringir la visibilitat el màxim possible a persones de la nostra confiança.

L'empresa ha de tractar una violació de la vida digital privada dels empleats com un incident de ciberseguretat propi, perquè és molt probable que el ciberatac pugui fer un moviment lateral i d'intrusió dintre de l'empresa.

### Instrucció 13

L'empresa ha de comunicar als empleats que convé restringir la publicació de dades personals, especialment les relatives a l'activitat professional dins l'empresa, i no permetre el funcionament de la geolocalització d'aquestes aplicacions quan s'estigui a les instal·lacions de l'empresa.

De la mateixa manera, cal conscienciar que la difusió de notícies falses, l'ús de llenguatge ofensiu, publicar dades personals de tercers i altres conductes poc ètiques poden vulnerar la llei i perjudicar reputacionalment l'empresa, que haurà de perseguir aquests tipus d'activitats quan afectin l'empresa o els seus membres.

## 8 Navegació segura

### Instrucció 14

Cal informar els empleats que, quan naveguin per internet, s'ha de revisar l'encriptació del canal amb la plana web (que l'URL tingui el símbol d'un cadenat) i, en casos de dubte, consultar el referent abans d'entrar-hi.

El teu navegador mostrarà el símbol d'un cadenat: revisa la informació que l'acompanya per a confirmar que s'ha establert un canal segur amb la plana web, que el certificat correspon a la web que estàs visitant i que no ha caducat, i sospita si trobes alguna cosa no familiar o habitual en la plana web que et mostra.

Les planes web utilitzen galetes per millorar l'experiència de l'usuari recordant les seves preferències i accelerant-ne l'ús, però poden també emprar-se per a altres motius poc ètics.

### Instrucció 15

S'ha de recomanar als empleats anul·lar per defecte la seva acceptació i revisar el contracte o avís que ofereixen i no confondre amb l'activació de notificacions que acostuma a aparèixer tot seguit a aquest avís. Que només acceptin les galetes que reconeguin i de les webs de confiança emprades habitualment: que la mandra no us jugui una mala passada.

### Instrucció 16

Cal recordar tancar la sessió correctament de les planes web visitades. En el cas que no hi hagi més opció que emprar equips de tercers, a més a més, activa la navegació privada o d'incògnit i elimina qualsevol historial/memòria cau del navegador un cop finalitzada la navegació

## On es pot obtenir informació addicional sobre ciberseguretat?

**La societat de la informació i el món digital també té els seus cossos de seguretat i autoritats que vetllen per la ciberseguretat.**

**A Catalunya hi ha l'Agència de Ciberseguretat de Catalunya:**
***https://ciberseguretat.gencat.cat/ca/inici***

**A Espanya hi ha el "Instituto Nacional de Ciberseguridad":**
***https://www.incibe.es***

**I a Europa hi ha la "European Union Agency for Cybersecurity":**
***https://www.enisa.europa.eu***

# Full de trucs

## Incidències de ciberseguretat

- Trucar al telèfon o escriure al correu de suport.

## Protegir les contrasenyes

- Poden ser l'única barrera d'accés a la informació.
- No repetir les contrasenyes en llocs diferents.
- No compartir la contrasenya.
- Memoritzar, no anotar, la teva contrasenya.
- Renovar les contrasenyes insegures.
- Els gestors de contrasenyes permeten una gestió còmoda.

## Contrasenya segura

- Mínim de 12 caràcters.
- Majúscules, minúscules, números i símbols.
- Evitar paraules de diccionari o combinacions numèriques.
- Revisar si alguna de les contrasenyes s'ha vist compromesa en alguna fuga d'informació o violació de seguretat i deixar-la d'utilitzar. Podeu consultar aquesta informació aquí: *https://haveibeenpwned.com*

## Protocol de creació de contrasenya complexa

- Partir d'una frase fàcil de recordar (cançó, poema, acudit). Per exemple:
  Una nit de lluna plena, tramuntàrem la carena = Undlp,tlc o 1ndlp,tlc
  De Barcelona a Mataró hi ha 40 quilòmetres? = DBaMhh40q?
  Vaig néixer el 1.970 a Manresa = Vne1.970aM
  El Pau va néixer el 6 i la Marta el 18 = EPvne6ilMe18

## Segon factor d'autenticació

- Verificació addicional al secret de la contrasenya. Incrementa significativament la seguretat dels accessos.

## Correu maliciós i de suplantació de la identitat

- L'estafa per robar informació als usuaris d'Internet arriba per xarxes socials, xat, e-mail, etc., falsificant les entitats conegudes.
- En cas de dubte, és millor verificar trucant per telèfon.

## Programari maliciós

- Evitar clicar enllaços desconeguts.
- No descarregar cap fitxer adjunt desconegut.
- No contestar un correu desconegut.
- Utilitzar només programes, apps i USB autoritzats.
- Actualitzar els equips personals i instal·lar un antivirus.

## Dispositius mòbils

- Protegir l'accés amb contrasenya o empremta.
- Configurar un bloqueig d'inactivitat.
- Xifrar la memòria del mòbil i fer còpia de seguretat.
- Mantenir actualitzat sistema i aplicacions.
- No instal·lar aplicacions desconegudes.
- Gestionar centralitzadament els mòbils propis.

## Xarxes socials

- No publicar dades que comprometin feina o persones.
- No publicar dades personals sense seguir els protocols.
- Revisar les opcions de privacitat dels perfils.
- Controlar els contactes que s'accepten.

## Navegació segura

- Vigilar webs falsos que es camuflen amb noms semblants.
- Revisar que la barra d'adreça tingui un cadenat (https).
- Evita introduir contrasenyes en ordinadors desconeguts.
- Tancar les sessions abans de tancar el navegador.
- Navegar en mode incògnit quan sigui possible.

# Autoavaluació

En aquest apartat s'ha creat un petit qüestionari d'autoavaluació que l'empresa pot fer servir per recordar alguns dels temes tractats a la fitxa pràctica de ciberseguretat i que poden ajudar-te a millorar la teva ciberseguretat

### Què hauries de fer si reps un correu que et sembla estrany i et demana obrir un fitxer Word?

- [ ] **1.** No obrir el Word
- [ ] **2.** Notificar una incidència
- [ ] **3.** Eliminar el correu electrònic
- [ ] **4.** Revisar si el remitent és de confiança

**Solucions:**

La resposta correcta és la (2). Perquè tot allò que et sembla estrany és molt valuós que ho notifiquis.

La (1) no és correcta perquè els correus maliciosos són perillosos pel simple fet de rebre'ls encara que no s'obri cap fitxer.

La (3) és incorrecta perquè l'acció d'eliminar el correu pot implicar que l'atacant rebi informació del teu ordinador. I, a més, es podrien perdre proves necessàries durant la investigació de la incidència.

La (4) és incorrecta perquè els remitents d'un correu electrònic són falsejables.

### Què faries si un company t'envia missatges de WhatsApp per comentar-te temes de la feina?

- [ ] **1.** No respondre
- [ ] **2.** Respondre dient-li que el WhatsApp no està permès
- [ ] **3.** Consultar si el WhatsApp és una aplicació autoritzada
- [ ] **4.** Comunicar-ho al referent de seguretat

**Solucions:**

La resposta correcta és la (3). Perquè s'ha de conèixer el lloc on consultar quines aplicacions són les autoritzades. Aquesta llista és viva i pot veure's modificada sovint.

La (1) no és correcta perquè, no fer res, no ajuda a millorar la ciberseguretat (si l'aplicació no està permesa).

La (2) és incorrecta perquè l'avaluació de quines accions són imprudents correspon a la comissió de seguretat de la informació.

La (4) és incorrecta perquè el comitè de seguretat ha confeccionat i publicat el llistat d'aplicacions permeses per resoldre aquest dubte.

A qui li consultaries per descobrir si es respecta la teva privacitat quan es monitoritza l'ús que realitzes del sistema d'informació?

- [ ] **1.** Al Delegat de Protecció de Dades
- [ ] **2.** Al referent de seguretat
- [ ] **3.** A l'Agència de Ciberseguretat de Catalunya
- [ ] **4.** A l'Autoritat Catalana de Protecció de Dades

**Solucions:**

La resposta correcta és la (1). Perquè la figura del Delegat de Protecció de Dades és la designada per l'empresa perquè actuï per defensar els drets digitals de les persones usuàries del sistema d'informació.

La (2) és incorrecta perquè la comissió de seguretat implementa mesures de ciberseguretat cercant la màxima seguretat tecnològica i escoltant les indicacions del Delegat de Protecció de Dades.

La (3) és incorrecta perquè l'Agència de Ciberseguretat de Catalunya no coneix el detall de les dades de caràcter personal que es tracten en el sistema de monitorització de l'empresa.

La (4) és incorrecta perquè l'Autoritat seria a qui hauries de recórrer si el Delegat de Protecció de Dades no atengués la teva consulta.

Què és millor: fer una contrasenya tan complicada que te l'hagis d'apuntar a tot arreu per recordar-la o fer una contrasenya simple per no tenir problemes de memòria?

- [ ] **1.** Fer una contrasenya simple i així només tenir-la al teu cap
- [ ] **2.** Fer una contrasenya complexa i protegir molt bé els papers on la tens anotada
- [ ] **3.** Cap de les dues primeres opcions
- [ ] **4.** Les dues primeres opcions són correctes si la contrasenya no la dius a ningú

**Solucions:**

La resposta correcta és la (3). Perquè la seguretat d'una contrasenya rau en un conjunt de circumstàncies. En aquest cas, tant que sigui difícil d'encertar com que sigui impossible de trobar escrita en cap nota de paper. El millor mecanisme d'autentificació és desconfiar de tenir només una contrasenya i incloure un segon factor d'autentificació.

La (1) és incorrecta perquè un ciberdelinqüent la podria encertar mitjançant una llista de contrasenyes possibles.

La (2) és incorrecta perquè els papers amb la contrasenya s'haurien de guardar amb una caixa forta i aleshores es convertiria en incòmode d'utilitzar.

La (4) és incorrecta perquè un atacant també la podria obtenir amb un atac d'enginyeria social, com per exemple el *phishing*.

### Si per teletreballar accedeixes al teu escriptori virtual, necessites un antivirus per a l'ordinador de casa?

- [ ] **1.** No
- [ ] **2.** Sí

**Solucions:**

La resposta correcta és la (2). Perquè un ordinador que accedeixi remotament l'escriptori virtual de l'empresa sense antivirus posa en risc la informació que s'obté mitjançant l'accés remot. Per exemple, el virus present a l'ordinador de casa podria copiar les contrasenyes d'accés que s'utilitzen o gravar tot el que aparegués en pantalla quan accedim l'escriptori virtual.

La (1) és incorrecta perquè l'antivirus de l'escriptori virtual només protegeix el que està passant dintre de l'aplicació d'escriptori virtual, però no en l'ordinador que utilitzem per saltar cap al teletreball.

### Consideres que tens prou coneixements tecnològics per protegir-te quan utilitzes Internet?

- [ ] **1.** Sí
- [ ] **2.** No

### Consideres que necessites formar-te per millorar les teves capacitats en ciberseguretat?

- [ ] **1.** Sí
- [ ] **2.** No

### Consideres que disposes de les eines suficients per protegir tecnològicament la informació?

- [ ] **1.** Sí
- [ ] **2.** No

### Consideres que són útils aquestes instruccions de la Fitxa de ciberseguretat de les TIC?

- [ ] **1.** Sí
- [ ] **2.** No

# NOTES

Can Muntanyola
Centre de Serveis
a les Empreses

**Contacta amb nosaltres si necessites suport:**
Granollers Mercat, Servei d'Empresa i Emprenedoria
Promoció Econòmica, Ajuntament de Granollers
Carrer Camí del Mig, 22, Polígon Palou Nord
08401 Granollers + 34 93 861 4783
***empresagm@granollers.cat***

***www.canmuntanyola.cat***

A la Plataforma GRID Granollers es pot trobar més informació, entre d'altres, sobre projectes cooperatius en aquest àmbit.
***www.gridgranollers.com***

Per a més informació sobre serveis relacionats amb la temàtica i/o d'altres oferts, podeu consultar el Catàleg de serveis a la indústria de Granollers Mercat en el següent enllaç:
***www.canmuntanyola.cat/programes-destacats/apunts-tecnics-per-la-industria.html***

Ajuntament Granollers

granollersmercat

Fitxes publicades:

**Autocosum**
**Servitització**
**Comptabilitat energètica**
**Quantificació ambiental**
**Transformació digital**
**Certificacions ambientals**
**Contractes Bilaterals**
**Cobertes amb fibrociment**
**Mobilitat sostenible**
**Ciberseguretat bàsica**

Properament:

Mesura i accés a dades de consum energètic
Gestió de la demanda

Elaborat amb la col·laboració de:

centralip

Amb el suport de:

Diputació Barcelona

Generalitat de Catalunya

Icones: Flaticon.com