# Guia per teletreballar amb seguretat

Consorci Administració Oberta de Catalunya AOC

A causa de l'estat d'alarma provocat pel coronavirus moltes administracions i organismos públics estan promovent el teletreball per garantir la continuïtat de les seves funcions i serveis. El teletreball, però, pot plantejar riscos de ciberseguretat sinó s'ha planificat amb temps, s'ha format adequadament al personal i s'ha configurat de forma segura els equips i les connexions. Atès el context actual, és possible que tot això no s'hagi pogut fer en molts casos; per aquest motiu us oferim una **selecció de les principals mesures de protecció bàsiques a tenir en compte** que us poden ajudar a teletreballar minimitzant els riscos de seguretat en el tractament de la informació de la vostra organització.

Tingueu present que la situació actual és molt atractiva per a "hackers" criminals per robar contrasenyes  i segrestar informació confidencial a canvi d'un rescat. Casos d'aquest tipus han succeït als darrers mesos en administracions públiques amb greu prejudici econòmic i de reputació.

Aquesta selecció s'ha elaborat amb l'objectiu de facilitar **una guia pràctica i executiva, adreçada a usuaris no experts d'administracions públiques mitjanes i petites, que no disposen de recursos** per aplicar un pla complert i avançat de seguretat. Volem evitar un excés d'informació i fer recomanacions no viables en les circumstàncies en què ens trobem. Per als usuaris que tingueu interès en aprofundir en aquest tema, facilitem enllaços addicionals al final de la guia.

Aquestes recomanacions són de caràcter general. Si la vostra organització disposa d'una guia de ciberseguretat pròpia feu cas d'aquesta.

## 1. Aspectes organitzatius

La teva organització és molt probable que ja disposi d'un protocol i responsable de ciberseguretat. Verifica amb ell els punts que t'oferim a continuació.

Segueix les instruccions de seguretat del **responsable tecnològic de la teva organització**

Fes ús de les **eines i aplicacions autoritzades per part de la teva organització**. Si tens la necessitat d'utilitzar altres solucions sigues prudent i utilitza només aplicacions de confiança.

I a més…

Valida que es realitzen còpies de seguretat dels documents corporatius que treballaràs des de casa.

Assabenta't bé de quin és el canal de comunicació d'incidències i de resolució de dubtes.

Notifica immediatament qualsevol incident de ciberseguretat al responsable tecnològic de la seva entitat.

2. Equip de treball

Des del teu equip de treball de casa tindràs accés a la informació confidencial de la teva organització. Tant si utilitzes un ordinador corporatiu, com un ordinador personal cal tenir en compte un conjunt de mesures de protecció i preventives. Si utilitzes un equip de treball corporatiu, el més habitual és que ja compleixi la majoria o la totalitat de les recomanacions a través de les polítiques de seguretat que ha forçat l'administrador.

Assegura't que el **sistema i les aplicacions estan actualitzades amb les darreres versions** i que l'actualització automàtica de versions està activada.

- Per a Windows
- Per a MAC

Comprova que el teu ordinador té un sistema d'**anti-virus i anti-malware actiu**.

- Per a Windows: activa Microsoft Defender Anti-malware
- Per a MAC: instal·la alguna solució de mercat amb una versió gratuïta: Kaspersky, Avast, AVG, Bitdefender, etc.

Aplica el **bloqueig automàtic de la pantalla** al cap de deu minuts.

I a més…

Crea en el teu sistema operatiu un compte independent per a la família i per a teletreballar. Cal evitar qualsevol accés no autoritzat a informació confidencial.

- Per Windows
- Per Mac

Activa un Tallafocs (firewall) al teu equip.

- Per Windows
- Per Mac.

3. Connexió a Internet i accés remot

Des del teu equip de treball de casa tindràs accés a la informació confidencial de la teva organització. Tant si utilitzes un ordinador corporatiu, com un ordinador personal cal tenir en compte un conjunt de mesures de protecció i preventives. Si utilitzes un equip de treball corporatiu, el més habitual és que ja compleixi la majoria o la totalitat de les recomanacions a través de les polítiques de seguretat que ha forçat l'administrador.

Evita utilitzar xarxes públiques WiFi que no siguin conegudes i de confiança per accedir remotament als serveis de l'organització.

I a més…

Utilitza, si escau, els serveis de connexió remota VPN (xarxa privada virtual) que recomani la teva organització per accedir als sistemes d'informació corporativa.

Comprova que el Router de connexió a Internet no utilitza la contrasenya per defecte de fàbrica. A Internet i YouTube trobareu molts tutorials. Us deixem el procediment que recomana l'Organització del Consumidor i Usuaris.

Configura la contrasenya del Router amb sistemes d'encriptació segura: WPA3 (preferentment) o WPA2.

## 4. Còpies de seguretat

Tota la documentació ofimàtica que generis a l'ordinador privat que facis servir per teletreballar i no sigui guardada al servidor de l'organització, segurament no disposarà d'un sistema de còpia de seguretat automatitzat. Per tant, és recomanable que prenguis la precaució de realitzar còpies de seguretat.

Fes còpies de seguretat dels documents generats en local a través d'algun dels següents mecanismes:

- Memòries USB: prèviament hauries d'haver netejat o formatejat per a garantir que no té cap risc
- Disc dur extern
- Servei d'emmagatzemament al núvol autoritzat per l'organització

## 5. Contrasenyes i autenticació

Des del teu equip de treball de casa tindràs accés a la informació confidencial de la teva organització. Tant si utilitzes un ordinador corporatiu, com un ordinador personal cal tenir en compte un conjunt de mesures de protecció i preventives. Si utilitzes un equip de treball corporatiu, el més habitual és que ja compleixi la majoria o la totalitat de les recomanacions a través de les polítiques de seguretat que ha forçat l'administrador.

Utilitza, sempre que sigui possible, l'accés als sistemes d'informació amb certificat digital (preferiblement T-CAT P) o sistemes d'autenticació de doble factor per a evitar que et robin la contrasenya. (Els sistemes de doble factor es basen en codis d'un sol ús que s'envien per SMS o bé a una APP)

Utilitza contrasenyes complexes: combinació de caràcters especials, números i lletres majúscules i minúscules.

No apuntis les contrasenyes corporatives enlloc.

Si instal·les certificats digitals en programari en el teu ordinador personal (TCAT-P, idCAT Certificat) utilitza l'opció "Escriure la Contrasenya per a la clau privada": d'aquesta forma només es podrà fer servir el certificat digital si es coneix la contrasenya.

I a més…

Si has d'utilitzar molts comptes amb diferents usuaris i contrasenya, utilitza una aplicació per a gestionar de forma segura les diferents contrasenyes. Hi ha diverses solucions que ofereixen una versió gratuïta (Lastpass, Dashlane, etc). Els dispositius Apple – iOS disposen d'un gestor de contrasenyes integrat amb el sistema operatiu.

6. Navegació segura per Internet

Des del teu equip de treball de casa tindràs accés a la informació confidencial de la teva organització. Tant si utilitzes un ordinador corporatiu, com un ordinador personal cal tenir en compte un conjunt de mesures de protecció i preventives. Si utilitzes un equip de treball corporatiu, el més habitual és que ja compleixi la majoria o la totalitat de les recomanacions a través de les polítiques de seguretat que ha forçat l'administrador.

Evitar la navegació per pàgines no segures i evitar la instal·lació de qualsevol programari o contingut dubtós.

I a més…

Els navegadors web dels mitjans hauran d'estar actualitzats i configurats amb la darrera versió i pegats de programari.

Eliminar periòdicament l'historial de navegació, les cookies, contrasenyes recordades i altres arxius temporals. Així evitem potencials elements espies.

7. Phishing

El phishing és un tipus de ciberdelicte que consisteix en l'enviament de correus fraudulents amb l'objectiu de robar la contrasenya o altra informació personal. És una de les estafes més utilitzades pels delinqüents informàtics. El funcionament del phishing és senzill: es rep un correu electrònic, amb una aparença legítima que demana actualitzar, validar o confirmar informació mitjançant un enllaç. Després de clicar en ell, se't redirigeix a una pàgina web falsa, en la qual es procedeix al robatori de la contrasenya o altres dades.

No facis clics a enllaços, ni descarreguis cap document adjunt de correus electrònics sospitosos. Sospita de correus electrònics que demanen fer actuacions no

habituals de renovar contrasenyes. Revisa l'adreça del remitent (no l'àlies) dels correus electrònics aparentment legítims.

I a més…

Quan et connectis via web verifica a la barra del navegador que l'adreça web del destí és la correcte. Els ciberdelinqüents poden replicar completament un web i robar-te la teva contrasenya.

8. A l'acabar la feina

Des del teu equip de treball de casa tindràs accés a la informació confidencial de la teva organització.

Tanca totes les connexions als sistemes d'informació i webs corporatives.

Fes una còpia de seguretat dels documents locals que has treballat i que no estan coberts per la còpia de seguretat corporativa.

I a més…

Elimina l'historial de navegació, les cookies, contrasenyes recordades i altres arxius temporals.

9. Més informació

Els usuaris que desitgin ampliar aquesta informació els recomanem que visitin les següents pàgines web especialitzades:

- Normes de ciberseguretat per a la prestació de serveis en la modalitat de teletreball
  Agència de Ciberseguretat de Catalunya
- Píndola “Ciberseguretat i protecció de dades”
  Escola d’Administració Pública de Catalunya
- Guía de seguridad en el teletrabajo
  Centre Seguretat TIC de la Comunitat Valenciana
- Teleworking Guidance: Best Practices, Sample Policies, and Cybersecurity
  University of North Carolina, School of Government
- Teleworking Quick Reference Guide
  California Cyber Security Integration Center
- CCN-CERT BP/18 Recomendaciones de Seguridad para situaciones de teletrabajo y refuerzo en vigilancia
  Centro Criptológico Nacional (contingut avançat)
- Cómo implantar una política de Acceso Remoto Seguro
  Centro Criptológico Nacional (contingut avançat)
- Guide to Enterprise Telework and Remote Access Security
  National Institute of Standards and Technology (contingut avançat)

Consorci Administració Oberta de Catalunya AOC