GUIA DE MESURES BÀSIQUES DE CIBERSEGURETAT

La Comissió de Tecnologia del Col·legi ha preparat aquest document amb diverses mesures bàsiques de ciberseguretat per protegir l'activitat professional.

Enric Mestre Ribera. Comissió de Tecnologia ICAVOR - Versió 2.6 (juny de 2022)

SUMARI

La Comissió de Tecnologia del Col·legi d'Advocats de Granollers, posa a la vostra disposició una "Guia de Mesures Bàsiques de Ciberseguretat" que ha elaborat per a tot tipus de nivell d'usuaris per ajudar a prevenir els riscos en ciberseguretat des d'un punt de vista professional i també personal.

RECOMANCIONS DE SEGURETAT GENERALS

NAVEGACIÓ SEGURA

Alhora d'introduir, enviar o consultar dades en línia revisar que el **lloc web tingui certificat SSL** (Secure Sockets Layer), és a dir, que l'accés web comenci per HTTPS, ja que protegeix les dades transferides mitjançant el xifratge activat per un certificat SSL en un servidor.

Verificar el nom dels destins web als quals et connectis. No és suficient confiar amb el disseny i la interfície sigui el mateix de sempre, perquè els ciberdelinqüents la podrien replicar per enganyar, estafar o roba dades. **Hi ha certificats d'alta seguretat, certifiquen el nom de domini i de l'empresa, són els certificats EV SSL**, aquesta informació es pot consultar des del navegador i són molt útils per evitar la suplantació de web en serveis tant sensibles com bancs i correu electrònic.

No ingressar a llocs que siguin potencialment perillosos o que hagen pogut ser compromesos. En aquest sentit, és molt recomanable la utilització de **programari antivirus que bloqui pàgines web que realitzen una activitat maliciosa.**

Bloquejar components de **Javascript** per defecte, solament habilitar aquells que confiem.

Important comprovar la **geolocalització el servidor de la web** (necessari a l'hora de valorar si un proveïdor ofereix garanties suficients de compliment RGPD):

- Introduir url web per saber la seva IP: https://www.wmtips.com/tools/info/
- Introduir núm. d'IP per saber a quin país s'allotja: https://www.ip2location.com/

  Si és país UE: OK RGPD

  País no UE: verificar si està sota sistema de nivell adequat de protecció que UE (Per exemple: AWS, Google, Microsoft Azure, etc...)

NAVEGADORS D'INTERNET

És recomanable utilitzar navegació privada (Inprivate), sobretot si s'utilitza **un ordinador compartit**. La navegació privada, és la manera de utilitzar internet en mode d'incògnit, i és una funció de privacitat en alguns navegadors web per a desactivar l'historial de navegació i la caixeta web on s'introdueixen dades, com les contrasenyes. Això permet a una persona navegar per la web sense emmagatzemar dades locals en l'historial del navegador i que podrien ser recuperats més tard.

La majoria de navegadors disposen d'aquesta opció, com ara:

- Brave (la finalitat d'aquest navegador bloqueja cookies i dades de seguiment)
- Chrome
- Edge
- Explorer
- Firefox
- Opera
- Safari
- Tor (té la finalitat del navegador és protegir la privacitat dels usuaris. També s'utilitza per la navegació del Deep Web o internet profunda).

EL MODE INCÒGNIT NO GARANTEIX EN ABSOLUT L'ANONIMAT A INTERNET.

Recomanacions:

- Mantenir el navegador i les seves extensions actualitzades.
- No instal·lar complements innecessaris o poc de confiança.

ÚS DE CONTRASENYES SEGURES

Les contrasenyes que s'utilitzin a internet han de ser robustes i diferents entre els diversos recursos que utilitzes a Internet. Utilitza números, lletres majúscules o minúscules, signes (%,;- etc..) i mínim de 12 caràcters.

No és recomanable utilitzar una mateixa contrasenya per diversos serveis i aplicacions, per tant, pot ser útil un gestor de contrasenyes per emmagatzemar-les i utilitzar un patró per generar-ne diverses.

Obtenir una bona contrasenya pots utilitzar generadors com per exemple el següent: https://www.lastpass.com/es/password-generator

IMPORTANT:

La pàgina web https://haveibeenpwned.com/ ens permet saber si les teves contrasenyes s'han vist compromeses per una bretxa de seguretat.

Podem tenir la millor contrasenya del món, però si el servei on està vinculada s'ha filtrat per un atac, tindrem un problema de seguretat addicional, ja que podem donar pistes o patró d'una manera de crear les contrasenyes, que poden utilitzar per entrar en d'altres comptes. Per evitar-ho, es recomanable utilitzar un gestor de contrasenyes.

QUÈ ÉS UN GESTOR DE CONTRASENYES?

Els gestors de contrasenyes són aplicacions que serveixen per a emmagatzemar les nostres credencials en una base de dades xifrada mitjançant una contrasenya mestra.

Mitjançant una extensió en el navegador, d'aquesta manera entrem en una web o aplicació que requereix contrasenya, la pròpia extensió ens la recordarà.

Gestors de Contrasenyes:

- https://www.lastpass.com/es
- https://1password.com/
- https://nordpass.com/es/

SEGONA AUTENTICACIÓ

Utilitzar com a mesura de seguretat una **segona d'autentificació per millorar el control d'accés remot**, per exemple en l'accés al correu electrònic o recursos de banca online, etc.

Amb aquest sistema t'assegures que malgrat t'encertin o et robin la contrasenya, també és necessari el teu dispositiu mòbil, targeta intel·ligent, clau USB, etc.

En algunes recursos web també recomanen utilitzar aplicacions per la doble autenticació, com per exemple:

- Google Authenticator
- Authy

WIFI

Evitar l'ús de xarxes wifi que no siguin confiança. Si no és imprescindible, no et connectis a xarxes públiques que no siguin conegudes ni autoritzades. El més recomanable és utilitzar la pròpia connexió 4G o 5G en el vostre dispositiu mòbil.

En el cas que no sigui possible i es necessiti una xarxa pública, connectar-se mitjançant VPN. Hi ha diverses opcions i serveis en el mercat.

Recomanem utilitzar una **contrasenya complexa i robusta en el vostre Wifi**, per evitar sabotatges externs.

ANTIVIRUS

Limita l'accés a Internet per prevenir contingut perillós. Això implica tenir un sistema **d'antivirus** activat i les aplicacions actualitzades a les darreres versions.

RECOMANACIÓ IMPORTANT:

En el cas d'haver-se infectat l'equip o dispositiu, recomanem canviar el més ràpid possible, totes les contrasenyes que tinguem emmagatzemades, com ara: Correu, bancs, xarxes socials, web, etc.

Mantenir actualitzat els equips, dispositius i aplicacions. Assegurat que el sistema d'actualització d'aplicacions i programes sigui l'habitual. La majoria d'aquestes actualitzacions són per millorar o corregir errors de seguretat.

AVÍS: Darrerament, s'han detectat atacs de ciberseguretat amb **actualitzacions falses de programari**. En cas de dubte esbrinar si les novetats proposades són correctes i legítimes. També en cas de dubte, es recomana posar-se en contacte amb el proveïdor per confirmar-ho la legitimitat de l'actualització.

VPN

Connexió remota segura utilitzant una VPN (Virtual Private Network).

Què és la VPN? és una xarxa privada virtual, mitjançant túnel segur entre el dispositiu i Internet, que assegurar la privacitat de les nostres dades.

Tipus VPN: softwares o mitjançant un aparell Firewall més programari.

És important protegir la nostra xarxa local amb connexió VPN, si **teletreballem i ens connectem remotament a un altre ordinador o servidor** (Per exemple connectar-se des de casa a terminal dels despatx).

CÒPIES DE SEGURETAT

És molt important realitzar periòdicament còpies de seguretat. Guardar-les en una ubicació diferent i alguna fora de la connexió a xarxa i verifica que es realitzen correctament. D'aquesta forma, en el cas de veure'ns afectats per algun incident de seguretat, podrem recuperar la informació i activitat d'una manera més àgil.

SERVEIS CLOUD O NÚVOL D'ARXIUS

En el cas que utilitzeu serveis cloud (One Drive, Dropbox, Drive, etc...), és recomanable **sincronitzar** els arxius i carpetes en un dispositiu, com a mesura de seguretat i còpia dels documents. Les condicions d'ús del servei, han de garantir de disponibilitat i confidencialitat de la informació.

L'advocat/da és responsable del tractament d'aquestes dades, està obligat a escollir proveïdors cloud que ofereixen garanties de compliment de la normativa de protecció de dades o inclús, que hagin estat validades i analitzades prèviament per l'autoritat de control (Per exemple: OneDrive i el paquet Office365 de Microsoft)

MESURES DE SEGURETAT GENERALS PEL CORREU ELECTRÒNIC

L'enviament de correus fraudulents és un dels problemes més greus en ciberseguretat, aquests pretenen que el receptor del missatge descarregui un document adjunt maliciós que podria infectar el seu equip o xarxa amb algun tipus de Malware per robar informació (contrasenyes, credencials bancaries, contactes, adreces, etc...) o bé utilitzar els contactes per enviar correu Spam o fins i tot amb la finalitat d'infectar-los.

Els missatges intenten enganyar-nos instant a revisar pressupostos, ofertes o ens demanen directament dades pròpies.

Dels correus maliciosos més perillosos són els ens poden infectar amb un **Ransonware.** Aquests encripten l'ordinador o ordinadors que estiguin connectats en una mateixa xarxa, demanat un rescat econòmic per poder-ho desencriptar. Normalment es realitzen en criptomònades i és impossible de rastrejar el pagament.

Recomanacions:

El correu d'ICAVOR utilitza la plataforma Office 365 de Microsoft, que és una de les més grans del món amb milions d'usuaris, on s'inverteix molts recursos fer frenar i evitar aquest tipus de correu. Tanmateix, és important si tenim el més mínim dubte que analitzem bé el correu. Per això, us recomanem el següent:

Aquests consells serveixen per a qualsevol tipus de dispositiu o sistema operatiu.

a. **No obris correus d'usuaris desconeguts o que no hagis sol·licitat**: elimina'ls directament. No contestis en cap cas a aquests correus.
b. **Revisa els enllaços** abans de fer clic encara que siguin de contactes coneguts.
c. **Desconfia dels enllaços escurçats**.
d. **Desconfia dels fitxers adjunts** encara que siguin de contactes coneguts.

   Recomanem el recurs https://www.virustotal.com/ que escanejar un document o URL amb més de 80 antivirus simultàniament.

e. **Tingues sempre actualitzat el sistema operatiu i l'antivirus**. En el cas de l'antivirus, comprova que està actiu.
f. En cas que **dubtis de la veracitat d'un correu**, posar-se en contacte amb el remitent per verificar que sigui autèntic. Us recomanem la Guia de "el Instituto Nacional de Seguirdad" per ajudar a identificar i verificar correus electrònics: https://www.incibe.es/protege-tu-empresa/blog/dudas-legitimidad-correo-aprende-identificarlos
g. **Verifica que el nom del remitent correspongui amb l'adreça de correu**. És un sistema bastant utilitzat per enganyar el receptor. Per exemple: remitent és el Col·legi Advocats Granollers però s'envia des de l'adreça: baldimir.7.7@ermail.ru
h. **Si el correu l'envia més d'un remitent o amb còpia vista, revisar que les adreces siguin correctes** i que no n'hagi cap d'estranya. Per exemple: col·legi@icavor.com ; baldimir.7.7@ermail.ru En aquest cas desconfia del missatge.
i. Sempre que sigui possible, utilitzar el correu en versió cloud, Exchange o Imap, en cas de virus o Ransonware en un dels nostres dispositius, que no afecti bústia correu que està en el servidor cloud, si més no, hi ha tindrem menys possibilitats que això passi.
j. **Filtres spam:** cada dia s'envien de 300 millons de correus SPAM a tot el món, alguns d'aquest amb virus. Per millorar la gestió del correu i ajudar els filtres antispam, els correus SPAM cal etiquetar-los com no desitjat. També es pot utilitzar els filtres dels gestors de correu per evitar aquells missatges molt repetitius s'enviïn a brossa directament. També es recomanable afegir els remitents més habituals o més important per nosaltres a com a correus segurs o llistes blanques. Així ens assegurem que sempre entrin en la safata d'entrada i no com a correu SPAM.

CONSELLS PER UTILITZAR EL DISPOSITIU MÒBIL

Sempre que sigui possible, els dispositius d'ús professional utilitzar-los només per tasques relacionades amb el treball i per usuaris autoritzats. **La instal·lació d'aplicacions personals podrien comprometre la confidencialitat d'informació de l'empresa.**

Recomanacions:

- Una correcta protecció i **bloqueig del dispositiu** amb mesures d'accés, com ara: utilitzar contrasenya, PIN, accés biomètric (empremta digital, etc). També bloquejar automàticament la pantalla del dispositiu passat uns segons sense utilitzar-lo.
- **Actualitzar** el sistema operatiu i aplicacions sempre que es requereixi. El propi mòbil i les aplicacions solen notificar que hi ha actualitzacions pendents. Sovint aquestes són millores i correccions de seguretat.
- Evitar l'ús de xarxes Wifi que no siguin confiança. Utilitzar la pròpia connexió 4G o 5G en el vostre dispositiu mòbil. En el cas que no sigui possible, es recomanable utilitzar una VPN
- Disposar d'un sistema de protecció en cas de pèrdua o robatori del dispositiu mòbil: geolocalitzar el mòbil, bloquejar-lo remotament i eliminar totes les dades. Aquest opció està disponible en els sistemes operatius com iOS i Android.
    - En Android disposa de les opcions: localització, bloqueig, eliminació de dades i fer sonar el mòbil encara que estigui en silenci. Més informació: https://myaccount.google.com/find-your-phone

UTILITZAR EL RECURSOS, SERVEIS WEB O APLICACIONS CONEGUDES I VERIFICADES

Vigilar i comprovar que les aplicacions que s'instal·len, siguin fiables i oficials. Per a disminuir la possibilitat de descarregar aplicacions falses o malicioses, us recomanem els següent:

- Què l'aplicació estigui verificada per la plataforma o market de les aplicacions
- Valoracions i comentaris dels usuaris
- Revisar els permisos de seguretat

DISCS DURS EXTERNS

Sempre que sigui possible, si necessitem mobilitat d'arxius, utilitzar plataformes cloud o de disc dur virtual, per evitar la possibilitat extraviar el dispositiu amb les conseqüències que poden esdevenir en pèrdua de dades, afectació i infracció en la privacitat dels clients. Recordeu que els advocats gestionen dades molt sensibles.

També evitem possibles infeccions de Virus i Malware si utilitzem el disc en dispositius que no són els nostres.

En el cas d'utilitzar discs durs externs es recomana encriptar-lo.

ENCRIPTACIÓ DE DOCUMENTS:

Xifrar una informació significa ocultar el contingut d'un missatge d'un document a simple vista. Això es fa mitjançant un algorisme matemàtic que modifica el text. Aquest només es pot desxifrà mitjançant una clau.

El contingut del document només el podran consultar els usuaris autoritzats.

És recomanable per informació que es comuniqui i contingui dades personals i/o amb contingut sensible (Per exemple: dades de categoria especial o de condemnes i infraccions penals).

SMS

SMS és un sistema de notificacions i avisos que utilitzem en el dia a dia i que també s'usen per enviar missatges maliciosos, on el remitent es fa passar per diferents empreses d'enviament i recepció de paqueteria i també d'entitats bancàries.

L'objectiu d'aquests SMS és que els seus destinataris facin clic en l'enllaç per executar una aplicació mòbil (Malware o troià) que es descarrega en el terminal mòbil facilitant d'aquesta manera l'accés a les dades de l'usuari, entre els quals es poder robar dades i claus bancàries. També s'enganya amb enllaços que suplanten webs verdaderes per que l'usuari escrigui les seves dades personals. Aquest engany és molt comú en missatges d'entitats bancàries.

Aquest sistema de SMS fraudulents es basa en la probabilitat, és a dir, en encertar amb situacions i serveis reals del destinatari, com ara el seu Banc o que estiguin esperant un paquet.

Mesures de protecció:

- Desconfiar del missatges genèrics. Les dades normalment són personalitzades amb informació del receptor. Per exemple: hem detectat que la targeta acabada 0000 ha fet un càrrec.
- Desconfiar dels missatges que demanen dades personals o fer login. Aquest tipus d'informació no es demana mai.
- Busquen enganyar la víctima amb missatges d'alerta. Per exemple: hem detectat que han utilitzat la seva targeta de crèdit de forma fraudulenta. Els missatge verdaders, sempre indican alguna dada personal, com la terminació de la targeta de crèdit.
- Molta atenció amb els missatges que s'acompanyen amb enllaços URL que s'assemblen a les reals per confondre i enganyar. Per exemple: bancosantande**rr**.com. També es recomanable verificar la web consultant el certificat SSL del HTTPS

(https://www.nomweb.com). En el cas que la web inici l'adreça web inicia amb HTTP desconfiar, segurament estaran suplantant una web verdadera.

- Desconfiar dels enllaços escurçats.
- Important: En cas de dubte trucar al remitent i preguntar si el missatge és autèntic.

APLICACIONS DE MISSATGERIA INSTANTÀNIA O XAT.

És un mitjà de comunicació molt estès i utilitzat en l'àmbit personal com professional. Els serveis de missatgeria més coneguts són:

- Whatsapp
- Telegram
- Signal
- Messenger
- Hangouts
- Teams, etc.

És recomanable utilitzar les aplicacions de missatgeria com a canal de comunicació a nivell informatiu, i no com a mitjà per a compartir dades personals o informació confidencial.

Quan utilitzem per finalitats professionals, cal informar prèviament sobre com es tractaran les dades (amb especial atenció als riscos derivats d'aquest tractament de dades) i sol·licitar el consentiment per poder dur a terme aquesta comunicació electrònica d'acord amb la normativa sobre comerç electrònic (LSSICE 34/2002) i, posar a disposició un sistema gratuït i fàcil per oposar-se a seguir rebent missatges i oposar-se al tractament de dades en sí. **També és recomanable fer còpies de seguretat dels missatges.**

Protegir l'accés aquestes aplicacions de missatgeria amb una contrasenya, PIN o mitjançant accés biomètric i també amb **activar notificacions per correu electrònic** quan s'accedeixi des d'un altre dispositiu.

Virus, Malware i estafes:

En les aplicacions de missatgeria com Whatsapp, també podem rebre missatges maliciosos amb l'objectiu d'estafar, infectar amb Virus o Malware per hackejar el telèfon mòbil. **Modus operandi:**

- Rebre un missatge per Whatsapp amb un codi de verificació, rebut suposadament per error des d'algun dels nostres contactes, ja que els criminals es valen del compte d'un número conegut per a suscitar la confiança de la seva víctima. Això vol dir que segurament el teu contacte l'han hackejat el seu compte. En aquest cas avisar ràpidament al remitent ja que li estan **suplantant la seva identitat**. Aquest sistema d'engany és molt utilitzat en **Grups de Whatsapp.** Aquest tipus de missatges simulen la verificació de dos passos demanen un codi de 4 a 6 xifres.
- Desconfiar de Whatsapp amb promocions i publicitat, sobretot si demanen dades personals o fer login.
- Desconfiar de enllaços escurçats

- Rebre missatges de contactes coneguts amb números de telèfon amb un prefix estranger.

VIDEOCONFERÈNCIES

No disposar de versions bàsiques, sinó apostar per versions professionals, ja que normalment aquestes disposen de les característiques que faran més segura la seva utilització. Per això, sempre és recomanable decantar-se per un pla empresarial verificant que compte amb les propietats necessàries per a fer un ús segur.

Cal tenir en compte, que els advocats tracten amb els seus clients dades personals especialment sensibles.

Recomanacions:

- Convidar els participants per correu electrònic i activar la sala d'espera a la reunió, que és un entorn previ a la reunió, per controla els assistents i per poder bloquejar les persones que no han estat convidades.
- Protegir l'accés a reunions amb un contrasenya, per evitar que terceres persones no autoritzades tinguin accés.
- Verificar que la plataforma de videoconferències s'adapti a la RGPD.

ALTRES RECURSOS RELACIONATS AMB LA CIBERSEGURETAT:

- https://ciberseguretat.gencat.cat/ca/actualitat/ Actualitat de l'Agència Catalan de Ciberseguretat.
- https://ciberseguretat.gencat.cat/ca/Recursos-de-Ciberseguretat-/index2.html Recursos de ciberseguretat de l'Agència Catalana de Ciberseguretat
- https://www.aepd.es/es (Agència Espanyola de Protecció de Dades)
- https://www.osi.es/es (Oficina de seguridad del internauta)
- https://www.osi.es/es/actualidad/avisos (avisos de seguretat)
- https://www.incibe.es/protege-tu-empresa/avisos-seguridad (Informació i avisos de seguretat de "el Instituto de Nacional de Ciberseguridad")
- Eines d'avaulació:
  - Avalua el teu Negoci: https://internetsegura.typeform.com/to/Sii3vN?source=22@&tipus=webMicrocurs
  - Protegeix-te del programari maliciós: https://internetsegura.typeform.com/to/Sx5LnXYC?source=22@&tipus=webMicrocurs
  - La informació a l'empresa: un tresor a protegir

https://internetsegura.typeform.com/to/ITDhKJMS?source=22@&tipus=webMicrocurs

- Dispositius de feina, a punt! https://internetsegura.typeform.com/to/emOraD?source=22@&tipus=webMicrocurs
- Còpies de seguretat, el pla A. https://internetsegura.typeform.com/to/IXUlpAuG?source=22@&tipus=webMicrocurs
- Ciberseguretat: sinònim de confiança https://internetsegura.typeform.com/to/Iz7nlZHK?source=22@&tipus=web