CIBERSEGURETAT

10 MESURES DE PROTECCIÓ

1 Instal·la un Antimalware i un Firewall al teu PC

Kaspersky, Bitdefender, McAfee, Sophos, Avast, AVG, Windows Defender.

2 Fes còpies de seguretat amb freqüència

Còpia seguretat de Windows, Time Machine de MAC, Duplicati, CloudBerry, Duplicacy, Uranium, Mozy, Cobian.

3 Xifra el disc del PC i els USB

- Navega sempre que puguis utilitzant https:// (moltes pàgines admeten tant http:// com https://) i assegura't que el certificat sigui correcte (Cadenat tancat).
- Utilitza sempre un Proxy VPN.
- Xifra els documents amb 7Zip, Encryppto.
- Xifra el disc del teu PC *(bitlocker(Windows), Veracrypt, FileVault(Mac).*
- Xifra els USB que utilitzis (*bitlocker, Veracrypt, Rohos Mini drive, USB Safeguard*).

4 Esborra les dades de forma segura

Per esborrar fitxers: *Eraser, Undelete360 i Portable data recovery.*
Per esborrar discos: *Darik's Boot And Nuke, (DBAN).*
Per recuperar fitxers esborrats: *Kickass Undelete.*

5 Manté el Sistema Operatiu actualitzat

Actualitza el SO, les aplicacions, el router wifi.

6 Utilitza el correu correctament

- Disposa d'un bon antispam.
- Xifra les dades sensibles.
- No participis en correus en cadena.
- No accedeixis als enllaços que et mostrin un correu electrònic.
- No obris els correus no sol·licitats o clarament falsos, les faltes d'ortografia poden ser una pista.
- Usa el malware online http://virusscan.jotti.org/
- Revisa les llistes negres https://mxtoolbox.com/blacklists.aspx

7 Navega per Internet de forma segura

- Utilitza pàgines segures (https://) sempre que sigui possible. Pàgines amb el cadenat o la barra de color verd.
- No descarreguis aplicacions gratuïtes que no tinguin garanties.
- Buscr el fabricant o web principal per fer una descàrrega, desconfia dels enllaços que reps per correu.
- Revisa el que el domini correspongui al lloc web on vols anar, fixa't bé en que el domini correspongui exactament al lloc on vols anar.
- Test d'infecció de pàgines web http://desenmascara.me/

8 Connecta't a Internet de forma segura

Si et connectes des d'una Web pública (Hotel, Aeroport, Starbucks,...), utilitza una VPN: NordVPN , GooseVPN, PureVPN , Private Internet Access, ExpressVPN.
Sistemes de VPN Gratuïts: Cyberghost, Hide.me, Opera VPN.

9 Utilitza i guarda els passwords de forma segura

Utilitza sempre password segurs:
- Més de 8 caràcters, majúscules, minúscules, número i símbols.
- Que no siguin paraules de diccionari.
- Passwords diferents per a cada servei.
- Escull les preguntes per recuperar el password amb compte.
- Activa els password de doble factor.
- Guarda els password de forma segura.

Per emmagatzemar els password: KeePass, Password safe, Password vault, LastPass.

10 Forma't i tingues cura de la seguretat

- Formació i conscienciació.
- No revelar els passwords a altres persones.
- Compte amb el que reps per email.
- En cas de dubte valida els fitxers amb un antivirus.
- Compte amb la informació sobre nosaltres que publiquis a Internet.
- Compte amb les metadades que contenen els documents.
- Compte amb les preguntes de recuperació de password.
- Llegeix bé els noms dels dominis.

D1G1CAB
IL·LUSTRE COL·LEGI DE L'ADVOCACIA DE BARCELONA
Comissió de Transformació Digital

CIBERSEGURIDAD

10 MEDIDAS DE PROTECCIÓN

1 Instala un Antimalware y un Firewall en tu PC

Kaspersky, Bitdefender, McAfee, Sophos, Avast, AVG, Windows Defender.

2 Haz copias de seguridad con frecuencia

Copia seguridad de Windows, Time Machine de MAC, Duplicati, CloudBerry, Duplicacy, Uranium, Mozy, Cobian.

3 Cifrado el disco del PC y los USB

- Navega siempre que puedas utilizando https:// (muchas páginas admiten tanto http:// como https://) y asegúrate que el certificado sea correcto (candado cerrado).
- Utiliza siempre un Proxy VPN.
- Cifra los documentos con 7Zip, Encryppto.
- Cifra el disco de tu PC *(bitlocker(Windows), Veracrypt, FileVault (Mac).*
- Cifra los USB que utilizas (bitlocker, Veracrypt, Rohos Mini drive, USB Safeguard)

4 Borra los datos de forma segura

Para borrar ficheros: *Eraser, Undelete360, Portable data recovery.*
Para borrar discos: *Darik's Boot And Nuke, (DBAN).*
Para recuperar ficheros borrados: *Kickass Undelete.*

5 Mantén el Sistema Operativo actualizado

Actualiza el SO, las aplicaciones, el router wifi.

6 Utiliza el correo correctamente

- Disponer de un buen antispam.
- Cifrar los datos sensibles.
- No participes en correos en cadena.
- No accedas a los enlaces que te muestren en un correo electrónico.
- No obras los correos no solicitados o claramente falsos, las faltas de ortografía pueden ser una pista.
- Análisis malware online http://virusscan.jotti.org/
- Revisión de listas negras https://mxtoolbox.com/blacklists.aspx

7 Navega por Internet de forma segura

- Utiliza páginas seguras (https://) siempre que sea posible. Páginas con el candado o la barra de color verde.
- No descargar aplicaciones gratuitas que no tengan garantías.
- Buscar el fabricante o web principal para hacer una descarga, desconfía de los enlaces que recibes por correo.
- Revisar que el dominio corresponda al lugar donde quieres ir, fíjate bien que el dominio corresponda exactamente al lugar que quieres visitar.
- Test infección de páginas web http://desenmascara.me/

8 Conéctate a Internet de forma segura

Si te conectas desde una Web pública (Hotel, Aeropuerto, Starbucks, ...), utiliza una VPN. NordVPN , GooseVPN, PureVPN , Private Internet Access, ExpressVPN.
Sistemas de VPN Gratuitos: Cyberghost, Hide.me, Opera VPN.

9 Utiliza y guarda los passwords de forma segura

Utiliza siempre password seguros:
- Más de 8 carácteres, mayúsculas, minúsculas, número y símbolos.
- Que no sean palabras de diccionario.
- Passwords diferentes por cada Servicio.
- Escoge las preguntas para recuperar el password con cuidado.
- Activa los password de doble factor.
- Guarda los password de forma segura.

Para almacenar los password: KeePass, Password safe, Password vault, LastPass.

10 Fórmate y ten cuidado de la seguridad

- Formación y concienciación.
- No revelar los passwords a otras personas.
- Cuidado con lo que recibes per email.
- En caso de duda validar los ficheros con un antivirus.
- Cuidado con la información sobre nosotros que publicamos en internet.
- Cuidado con los metadatos que contienen los documentos.
- Cuidado con las preguntas de recuperación de password.
- Lee bien los nombres de los dominios.

D1G1CAB
IL·LUSTRE COL·LEGI DE L'ADVOCACIA DE BARCELONA
Comisión de Transformación Digital