DIPUTACIÓ DE VALÈNCIA

Protecció de Dades i Seguretat de la Informació

Butlletí protecció de dades

Butlletí del Departament de protecció de dades i Seguretat de la Informació de la Diputació Provincial de València

Butlletí N.º 18| Desembre 2021

SEGURETAT EN LA NAVEGACIÓ WEB

ÍNDEX

SEGURETAT EN LA NAVEGACIÓ WEB

Us convidem a traslladar-nos aquelles temàtiques que resulten del vostre interés per als pròxims butlletins informatius. Aquestes peticions hauran de dirigir-se a:

Diputació de València

Dpt. de Protecció de Dades s Seguretat de la Informació

Pl. de Manises, 4 46003 Valencia

email: dpdsi@dival.es

SUSCRIPCIONS

Si desitges subscriure's al nostre Butlletí informatiu accedeix al següent enllaç

INTRODUCCIÓ

En l'actualitat, un dels recursos més utilitzats en el dia a dia de qualsevol organització és el de la navegació web, la qual cosa ens permet buscar informació, accedir el correu electrònic i realitzar multitud de tasques que ens faciliten la nostra labor en l'organització.

No obstant això, en la navegació web es donen pràctiques que poden suposar un vertader risc per a la privacitat i seguretat de les dades que alberga la nostra organització. A causa de la gran quantitat d'informació que gestionen els navegadors web, aquests són un objectiu potencial per als ciberdelinqüents.

Per això, serà crucial per a la nostra organització que els usuaris dels sistemes d'informació adopten una sèrie de mesures de seguretat i privacitat que reduïsquen al mínim l'exposició, tant dels usuaris com de la pròpia organització.

En el butlletí informatiu d'aquest mes, es faciliten una sèrie de pautes per a una navegació segura.

"EN LA NAVEGACIÓ WEB ES DONEN PRÀCTIQUES QUE PODEN SUPOSAR UN VERTADER RISC PER A LA PRIVACITAT I SEGURETAT DE LES DADES QUE ALBERGA LA NOSTRA ORGANITZACIÓ. A CAUSA DE LA GRAN QUANTITAT D'INFORMACIÓ QUE GESTIONEN ELS NAVEGADORS WEB, AQUESTS SÓN UN OBJECTIU POTENCIAL PER ALS CIBERDELINQÜENTS".

RECOMANACIONS PER A UNA NAVEGACIÓ WEB SEGURA

ACTUALITZACIÓ DEL NAVEGADOR

Els navegadors (Google Chrome, Mozilla Firefox, Microsoft Edge, Internet Explorer, Safari, Opera, etc.) estan exposats a fallades de seguretat que poden obrir la porta al fet que individus maliciosos accedisquen a la nostra informació o prenguen el control dels nostres dispositius. Ara bé, si el navegador es troba actualitzat a la seua última versió, comptarà amb els pegats de seguretat necessaris per a corregir les vulnerabilitats que s'hagueren descobert. Per tant, hem de mantindre-ho actualitzat, preferiblement a través de l'opció d'actualitzacions automàtiques. Aquesta funcionalitat ve incorporada pels principals navegadors.

EXTENSIONS O COMPLEMENTS

Les extensions, també conegudes com a complements o *add-ons*, són eines que atorguen als navegadors web funcionalitats extra que per defecte no tenen. Existeixen multitud d'aplicacions d'aquest tipus amb una gran varietat de funcionalitats que poden anar des de bloquejar finestres emergents o gestionar les contrasenyes fins a, simplement, canviar la imatge de fons del navegador.

Afegir extensions en els navegadors pot arribar a suposar un risc per a la seguretat de l'organització. A vegades, la instal·lació d'aquestes extensions requereix que l'usuari atorgue una sèrie de permisos, com per exemple, llegir i modificar el contingut de les webs que es visiten. El funcionament d'aquests permisos és limitat, ja que si no s'accepten, no es permet la seua instal·lació. Però alguns complements, per inofensius que semblen, podrien dur a terme activitats malicioses.

Per aquest motiu, és recomanable seguir una sèrie de recomanacions abans d'instal·lar una aplicació d'aquestes característiques:

- Instal·lar únicament els complements que siguen necessaris per a l'acompliment de l'activitat en l'organització.
- Utilitzar únicament les botigues oficials que disposen els navegadors, ja que abans de publicar-se, aquestes han sigut comprovades perquè no realitzen activitats malicioses, encara que no es tracta d'una mesura definitiva.
- Comprovar els comentaris dels usuaris i verificar que aquests no adverteixen sobre activitats fraudulentes de l'extensió.
- Si es va instal·lar en el seu moment una extensió per a una certa tasca que ja no siga d'utilitat, el millor serà desinstal·lar-la o, almenys, deshabilitar-la fins que es torne a necessitar.

PROTOCOL SEGUR: HTTPS

HTTPS (Protocol de Transferència de Hiper-Text) és un protocol que permet establir una connexió segura entre el servidor i el client, que no pot ser interceptada per persones no autoritzades. Es recomana visitar webs amb el Protocol HTTPS (https://www.xxxxxxx.es/) enfront d'HTTP (https://www.xxxxxxx.es/).

CREDENCIALS D'ACCÉS

Els navegadors compten amb una funció d'autocompletat de credencials d'accés, la qual simplifica l'accés als serveis que requereixen d'usuari i contrasenya. No obstant això, utilitzar aquesta funció no és recomanable ja que davant un accés no autoritzat al dispositiu, els serveis que compten amb les credencials emmagatzemades seran també vulnerables. Bastaria que l'atacant obrira el servei en qüestió en el navegador i la funció d'autocompletat de credencials faria la resta.

Es recomana no emmagatzemar contrasenyes de manera predeterminada per mitjà del navegador i utilitzar eines més segures per a aquesta gestió (per exemple, gestors de contrasenyes que implementen un sistema de xifratge robust).

SEGUIMENT DE L'ACTIVITAT DE NAVEGACIÓ

En utilitzar internet es donen pràctiques que afecten la nostra privacitat, com és el cas del seguiment de l'activitat de navegació que es produeix en visitar un gran nombre de pàgines webs. Aquest seguiment, habitualment, es duu a terme a través de les denominades *cookies*, xicotets fitxers que guarden informació dels llocs que visites, principalment amb finalitats publicitaris o estadístics. L'objectiu que persegueixen és l'elaboració de perfils per a oferir publicitat ajustada als interessos i característiques concretes de cada individu, a més de recopilar informació estadística d'accés als serveis web.

Si, en visitar un lloc web, et sol·liciten el consentiment per a l'ús de cookies , no el facilites. També pots configurar el navegador per a bloquejar les *cookies*.

XARXES WIFI PÚBLIQUES

Com advertíem en butlletins anteriors, quan naveguem per Internet connectats a una xarxa Wifi pública, desconeixem qui és l'administrador o quines mesures de seguretat utilitza per a impedir accions malintencionades d'altres usuaris connectats i, per tant, podem exposar-nos a una sèrie de riscos: robatori de dades transmeses o emmagatzemades en el dispositiu,

infecció del dispositiu, etc.

És preferible que, en comptes de connectar-te a xarxes sense fils obertes, et connectes a la xarxa 3G/4G/5G de l'operador. En cas de necessitat, si et connectaràs a una xarxa sense fil pública, és preferible accedir a una xarxa amb seguretat WPA o WPA2. Les xarxes obertes i amb seguretat WEP són totalment insegures. Pots consultar els detalls de la xarxa WIFI per a comprovar davant quina mena de xarxa et trobes.

TANCAR SESSIÓ

Tanca sempre la sessió quan isques d'una pàgina en la qual t'hages autenticat amb usuari i contrasenya. Amb aquesta acció evitaràs que, si una persona utilitza el teu ordinador o el teu dispositiu mòbil, puga accedir a la teua informació personal usant la sessió que has deixat oberta.

RECORDA:

EN NAVEGAR PER LA WEB…

- Assegura't que el **navegador web** que utilitzes es troba **actualitzat** a la seua última versió.
- Instal·la únicament els **complements o extensions** que siguen **necessaris** per a l'acompliment de l'activitat en l'organització i fes-lo des de les **botigues oficials** que disposen els navegadors.
- **Desinstal·la** o, almenys, **deshabilita**, els **complements o extensions que no utilitzes.**
- Intenta visitar webs que utilitzen el **Protocol HTTPS** (https://www.xxxxxxx.es/).
- Si, en visitar un lloc web, et sol·liciten el consentiment per a l'ús de cookies , **no** el facilites, o configura el navegador per a bloquejar **les cookies**.
- **No emmagatzemes contrasenyes** de manera predeterminada per mitjà del navegador.
- **No et connectes a xarxes sense fils obertes**. En cas de necessitat, si et connectaràs a una xarxa sense fil pública, és preferible accedir a una xarxa amb seguretat WPA o WPA2. Pots consultar els detalls de la xarxa WIFI per a comprovar davant quina mena de xarxa et trobes.
- **Tanca sempre la sessió** quan isques d'una pàgina en la qual t'hages autenticat amb usuari i contrasenya.

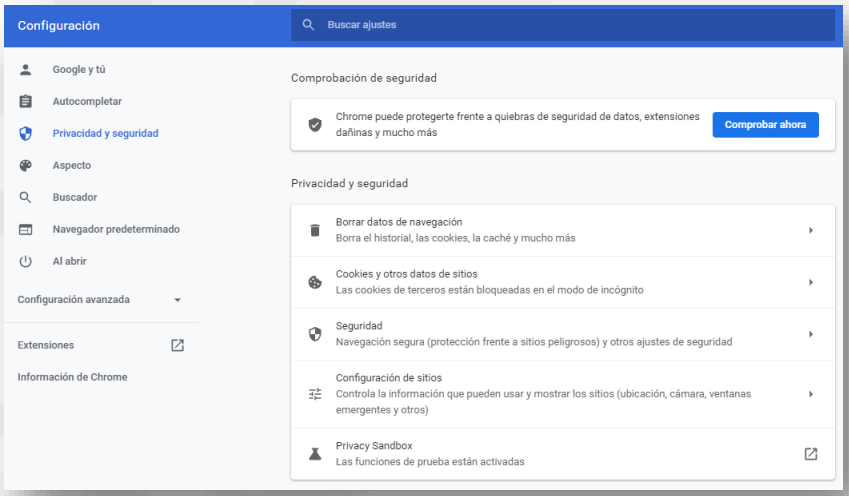
OPCIONS DE SEGURETAT I PRIVACITAT DELS NAVEGADORS WEB

Actualment, els navegadors permeten configurar determinades opcions de seguretat i privacitat: no acceptar cookies de tercers, bloquejar pop-ups, evitar la sincronització de contrasenyes, evitar l'autocompletat, esborrar els fitxers temporals i cookies en tancar el navegador, bloquejar la geolocalització, etc.

T'animem que revises les opcions de configuració del navegador que utilitzes habitualment i al fet que habilites o deshabilites aquelles que consideres més interessants per a protegir la teua privacitat i mantindre segura la informació de l'organització. Et vam mostrar la ruta d'accés a les mateixes en alguns dels navegadors més utilitzats:

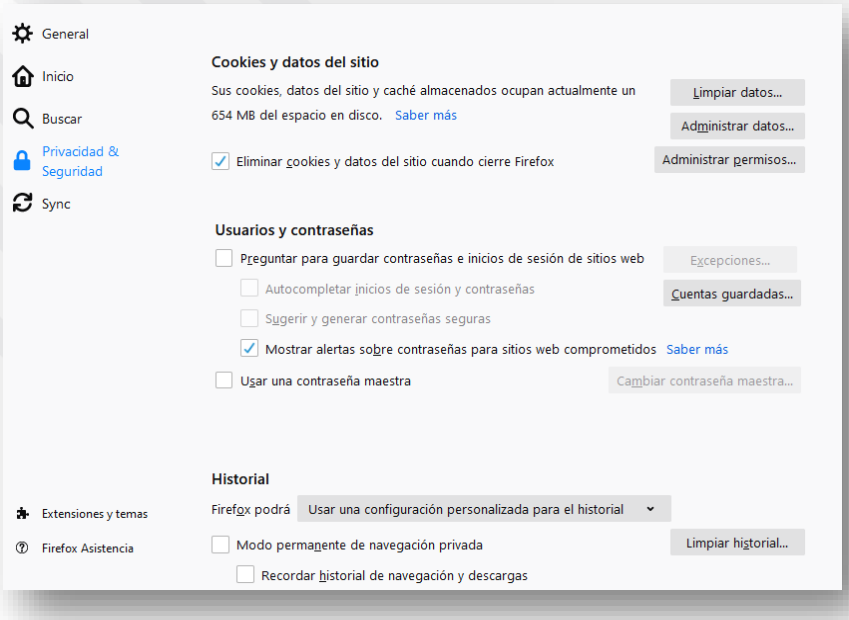
OPCIONS DE PRIVACITAT I SEGURETAT DE GOOGLE CHROME

Menú > Configuració > Privacitat i seguretat



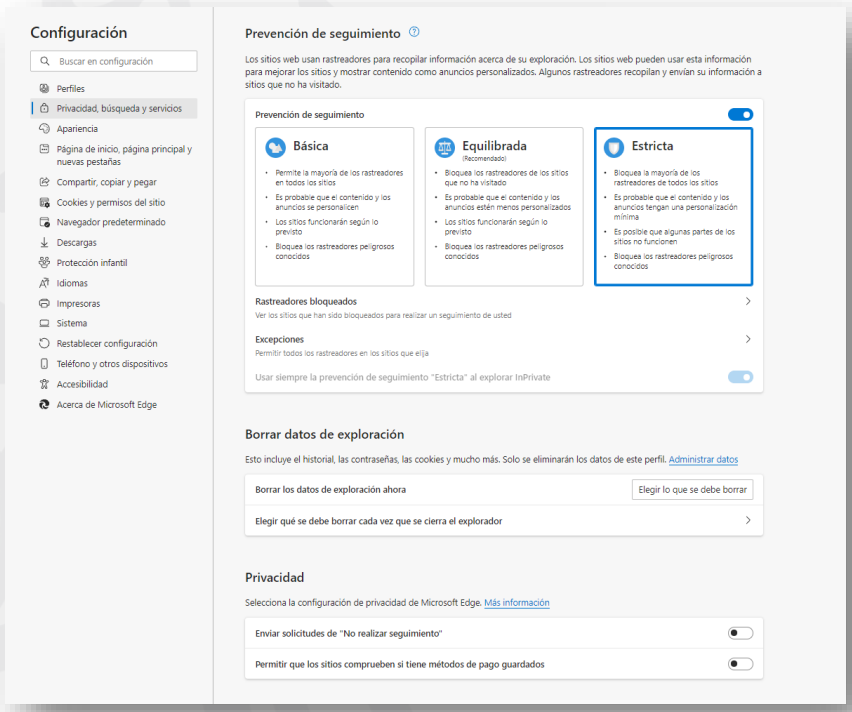
OPCIONS DE PRIVACITAT I SEGURETAT DE MOZILLA FIREFOX

Menú > Opcions > Privacitat & Seguretat



OPCIONS DE PRIVACITAT I SEGURETAT DE MICROSOFT EDGE

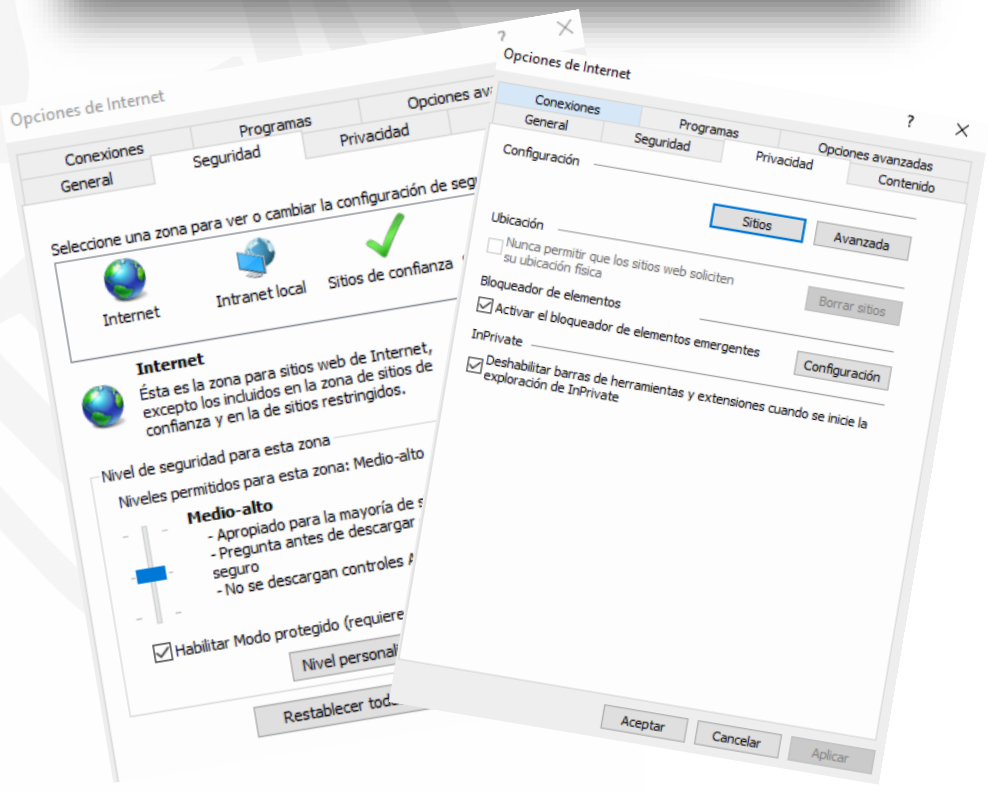
Menú > Configuració > Privacitat, cerca i serveis



OPCIONS DE PRIVACITAT I SEGURETAT D'INTERNET EXPLORER

Eines> Opcions d'Internet > Seguretat

Eines> Opcions d'Internet > Privacitat



"REVISA LES OPCIONS DE PRIVACITAT I SEGURETAT DEL NAVEGADOR WEB QUE UTILITZES HABITUALMENT"

MATERIAL COMPLEMENTARI

- Informe: Seguretat i riscos dels navegadors web (CCN). Consulta aquest enllaç.
- Guia: Privacitat i Seguretat en Internet (AEPD, INCIBE, OSI). Consulta aquest enllaç.
- Nota Tècnica: Mesures per a minimitzar el seguiment en internet (AEPD). Consulta aquest enllaç
- Infografia: Mesures per a minimitzar el seguiment en internet (AEPD). Consulta aquest enllaç.
- Blog: Navegació privada per a tu i per a la teua empresa. Part I (INCIBE). Consulta aquest enllaç.
- Blog: Navegació privada per a tu i per a la teua empresa. Part II (INCIBE). Consulta aquest enllaç.
- Blog: Riscos en l'ús d'extensions per als navegadors i mesures de seguretat (INCIBE). Consulta aquest enllaç.
- Blog: Navegadors (OSI). Consulta aquest enllaç.
- Blog: Esborrant el rastre que deixes en usar el navegador (OSI). Consulta aquest enllaç.

NOTÍCIES

- **Entra en vigor el Reial decret llei 24/2021, de 2 de novembre, que transposa directives de la Unió Europea en determinades matèries com la relativa a les dades obertes i la reutilització de la informació del sector públic.** El Llibre tercer de l'incorpora a l'ordenament jurídic espanyol les novetats de la Directiva (UE) 2019/1024 del Parlament Europeu i del Consell, de 20 de juny de 2019, relativa a les dades obertes i la reutilització de la informació del sector públic. Consulta la norma en aquest enllaç.

- **L'AEPD ens parla en el seu Blog dels recursos per a tractar d'evitar la publicitat no desitjada.** El correu postal, la bustiada, les trucades al telèfon fix o la venda porta a porta han sigut substituïdes en la seua gran majoria per correus electrònics, missatges de text i les especialment molestes trucades al telèfon mòbil. Diferent normativa, inclosa la relacionada amb la protecció de dades, ens protegeix de determinades pràctiques comercials en línia i offline, però existeixen uns certs hàbits o accions preventives que podem dur a terme per a tractar d'evitar la molesta publicitat no desitjada o spam. Consulta el Blog en aquest enllaç.

- **L'AEPD sanciona a la Conselleria d'Educació del Principat d'Astúries per no utilitzar protocol segur en el seu web i per incorporar un apartat de "Treballa amb nosaltres" sense donar compliment a la Llei de Serveis de la Societat de la Informació.** En el procediment instruït per l'AEPD a la Conselleria d'Educació del Principat d'Astúries, titular i responsable de la pàgina web en qüestió, se sanciona a la citada Conselleria per entendre que la pàgina no és segura, perquè utilitza el protocol http://; així com per considerar que no compleix amb la Llei de Serveis de la Societat de la Informació, en considerar a la mateixa "prestador de serveis de la societat de la informació", perquè a través d'aquesta web es gestionava la borsa de treball de l'Institut, possibilitant als usuaris enviar les seues dades personals i el seu curriculum vitae directament al centre educatiu. Consulta la Resolució en aquest enllaç.