DIPUTACIÓ DE VALÈNCIA

Protecció de Dades i Seguretat de la Informació

Boletín protección de datos

Boletín del Departamento de protección de datos y Seguridad de la Información de la Diputación Provincial de Valencia

Boletín N.º 18| Diciembre 2021

SEGURIDAD EN LA NAVEGACIÓN WEB

Í N D I C E

SEGURIDAD EN LA NAVEGACIÓN WEB

Os invitamos a trasladarnos aquellas temáticas que resulten de vuestro interés para los próximos boletines informativos. Estas peticiones deberán dirigirse a:

Diputación de Valencia

Dpto. de Protección de Datos y Seguridad de la Información

Pl. de Manises, 4 46003 Valencia

email: dpdsi@dival.es

SUSCRIPCIONES

Si deseas suscribirse a nuestro Boletín informativo accede al siguiente enlace

INTRODUCCIÓN

En la actualidad, uno de los recursos más utilizados en el día a día de cualquier organización es el de la navegación web, lo que nos permite buscar información, acceder el correo electrónico y realizar multitud de tareas que nos facilitan nuestra labor en la organización.

No obstante, en la navegación web se dan prácticas que pueden suponer un verdadero riesgo para la privacidad y seguridad de los datos que alberga nuestra organización. Debido a la gran cantidad de información que gestionan los navegadores web, estos son un objetivo potencial para los ciberdelincuentes.

Por ello, será crucial para nuestra organización que los usuarios de los sistemas de información adopten una serie de medidas de seguridad y privacidad que reduzcan al mínimo la exposición, tanto de los usuarios como de la propia organización.

En el boletín informativo de este mes, se facilitan una serie de pautas para una navegación segura.

"EN LA NAVEGACIÓN WEB SE DAN PRÁCTICAS QUE PUEDEN SUPONER UN VERDADERO RIESGO PARA LA PRIVACIDAD Y SEGURIDAD DE LOS DATOS QUE ALBERGA NUESTRA ORGANIZACIÓN. DEBIDO A LA GRAN CANTIDAD DE INFORMACIÓN QUE GESTIONAN, LOS NAVEGADORES WEB SON UN OBJETIVO POTENCIAL PARA LOS CIBERDELINCUENTES".

RECOMENDACIONES PARA UNA NAVEGACIÓN WEB SEGURA

ACTUALIZACIÓN DEL NAVEGADOR

Los navegadores (Google Chrome, Mozilla Firefox, Microsoft Edge, Internet Explorer, Safari, Opera, etc.) están expuestos a fallos de seguridad que pueden abrir la puerta a que individuos maliciosos accedan a nuestra información o tomen el control de nuestros dispositivos. Ahora bien, si el navegador se encuentra actualizado a su última versión, contará con los parches de seguridad necesarios para corregir las vulnerabilidades que se hubieran descubierto. Por tanto, hemos de mantenerlo actualizado, preferiblemente a través de la opción de actualizaciones automáticas. Esta funcionalidad viene incorporada por los principales navegadores.

EXTENSIONES O COMPLEMENTOS

Las extensiones, también conocidas como complementos o *add-ons*, son herramientas que otorgan a los navegadores web funcionalidades extra que por defecto no tienen. Existen multitud de aplicaciones de este tipo con una gran variedad de funcionalidades que pueden ir desde bloquear ventanas emergentes o gestionar las contraseñas hasta, simplemente, cambiar la imagen de fondo del navegador.

Añadir extensiones en los navegadores puede llegar a suponer un riesgo para la seguridad de la organización. En ocasiones, la instalación de estas extensiones requiere que el usuario otorgue una serie de permisos, como por ejemplo, leer y modificar el contenido de las webs que se visitan. El funcionamiento de estos permisos es limitado, ya que si no se aceptan, no se permite su instalación. Pero algunos complementos, por inofensivos que parezcan, podrían llevar a cabo actividades maliciosas.

Por este motivo, es recomendable seguir una serie de recomendaciones antes de instalar una aplicación de estas características:

- Instalar únicamente los complementos que sean necesarios para el desempeño de la actividad en la organización.
- Utilizar únicamente las tiendas oficiales que disponen los navegadores, ya que antes de publicarse, estas han sido comprobadas para que no realicen actividades maliciosas, aunque no se trata de una medida definitiva.
- Comprobar los comentarios de los usuarios y verificar que estos no advierten sobre actividades fraudulentas de la extensión.
- Si se instaló en su momento una extensión para una cierta tarea que ya no sea de utilidad, lo mejor será desinstalarla o, al menos, deshabilitarla hasta que se vuelva a necesitar.

PROTOCOLO SEGURO: HTTPS

HTTPS (Protocolo de Transferencia de Hiper-Texto) es un protocolo que permite establecer una conexión segura entre el servidor y el cliente, que no puede ser interceptada por personas no autorizadas. Se recomienda visitar webs con el Protocolo HTTPS (https://www.xxxxxxx.es/) frente a HTTP (https://www.xxxxxxx.es/).

CREDENCIALES DE ACCESO

Los navegadores cuentan con una función de autocompletado de credenciales de acceso, la cual simplifica el acceso a los servicios que requieren de usuario y contraseña. No obstante, utilizar esta función no es recomendable ya que ante un acceso no autorizado al dispositivo, los servicios que cuentan con las credenciales almacenadas serán también vulnerables. Bastaría con que el atacante abriese el servicio en cuestión en el navegador y la función de autocompletado de credenciales haría el resto.

Se recomienda no almacenar contraseñas de forma predeterminada por medio del navegador y utilizar herramientas más seguras para dicha gestión (por ejemplo, gestores de contraseñas que implementen un sistema de cifrado robusto).

SEGUIMIENTO DE LA ACTIVIDAD DE NAVEGACIÓN

Al utilizar internet se dan prácticas que afectan a nuestra privacidad, como es el caso del seguimiento de la actividad de navegación que se produce al visitar un gran número de páginas webs. Este seguimiento, habitualmente, se lleva a cabo a través de las denominadas *cookies*, pequeños ficheros que guardan información de los sitios que visitas, principalmente con fines publicitarios o estadísticos. El objetivo que persiguen es la elaboración de perfiles para ofrecer publicidad ajustada a los intereses y características concretas de cada individuo, además de recopilar información estadística de acceso a los servicios web.

Si, al visitar un sitio web, te solicitan el consentimiento para el uso de *cookies*, no lo facilites. También puedes configurar el navegador para bloquear las *cookies*.

REDES WIFI PÚBLICAS

Como advertíamos en boletines anteriores, cuando navegamos por Internet conectados a una red WiFi pública, desconocemos quién es el administrador o qué medidas de seguridad utiliza para impedir acciones malintencionadas de otros usuarios conectados y, por tanto, podemos exponernos a una serie de riesgos: robo de datos transmitidos o almacenados en

el dispositivo, infección del dispositivo, etc.

Es preferible que, en vez de conectarte a redes inalámbricas abiertas, te conectes a la red 3G/4G/5G del operador. En caso de necesidad, si vas a conectarte a una red inalámbrica pública, es preferible acceder a una red con seguridad WPA o WPA2. Las redes abiertas y con seguridad WEP son totalmente inseguras. Puedes consultar los detalles de la red WIFI para comprobar ante qué tipo de red te encuentras.

CERRAR SESIÓN

Cierra siempre la sesión cuando salgas de una página en la que te hayas autenticado con usuario y contraseña. Con esta acción evitarás que, si una persona utiliza tu ordenador o tu dispositivo móvil, pueda acceder a tu información personal usando la sesión que has dejado abierta.

RECUERDA:

AL NAVEGAR POR LA WEB…

- Asegúrate de que el **navegador web** que utilices se encuentra **actualizado** a su última versión.
- Instala únicamente los **complementos o extensiones** que sean **necesarios** para el desempeño de la actividad en la organización y hazlo desde las **tiendas oficiales** que disponen los navegadores.
- **Desinstala** o, al menos, **deshabilita**, los **complementos o extensiones que no utilices.**
- Intenta visitar webs que utilicen el **Protocolo HTTPS** (https://www.xxxxxxx.es/).
- Si, al visitar un sitio web, te solicitan el consentimiento para el uso de **cookies**, **no** lo facilites, o configura el navegador para **bloquear las cookies**.
- **No almacenes contraseñas** de forma predeterminada por medio del navegador.
- **No te conectes a redes inalámbricas abiertas**. En caso de necesidad, si vas a conectarte a una red inalámbrica pública, es preferible acceder a una red con seguridad WPA o WPA2. Puedes consultar los detalles de la red WIFI para comprobar ante qué tipo de red te encuentras.
- **Cierra siempre la sesión** cuando salgas de una página en la que te hayas autenticado con usuario y contraseña.

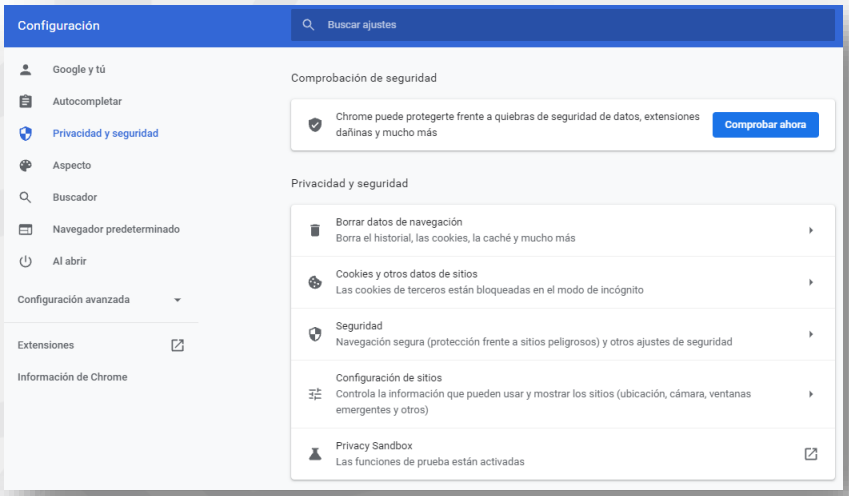
OPCIONES DE SEGURIDAD Y PRIVACIDAD DE LOS NAVEGADORES WEB

Actualmente, los navegadores permiten configurar determinadas opciones de seguridad y privacidad: no aceptar cookies de terceros, bloquear pop-ups, evitar la sincronización de contraseñas, evitar el autocompletado, borrar los ficheros temporales y cookies al cerrar el navegador, bloquear la geolocalización, etc.

Te animamos a que revises las opciones de configuración del navegador que utilices habitualmente y a que habilites o deshabilites aquellas que consideres más interesantes para proteger tu privacidad y mantener segura la información de la organización. Te mostramos la ruta de acceso a las mismas en algunos de los navegadores más utilizados:

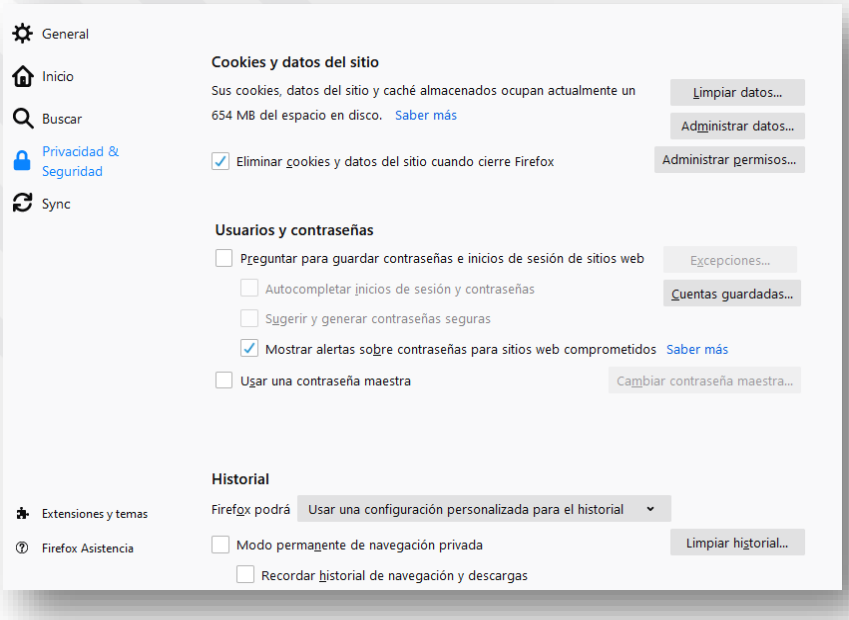
OPCIONES DE PRIVACIDAD Y SEGURIDAD DE GOOGLE CHROME

Menú > Configuración > Privacidad y seguridad



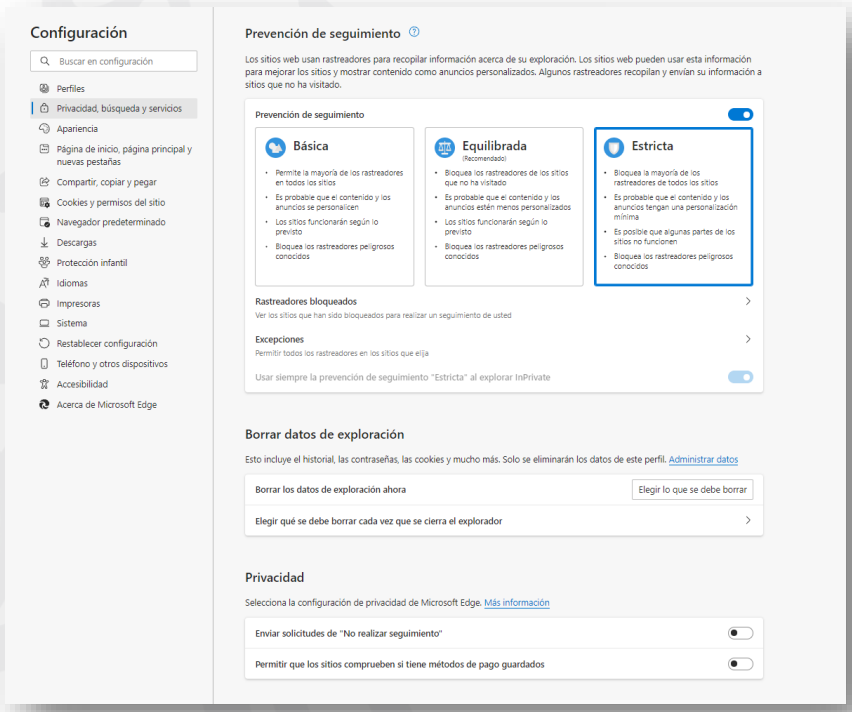
OPCIONES DE PRIVACIDAD Y SEGURIDAD DE MOZILLA FIREFOX

Menú > Opciones > Privacidad & Seguridad



OPCIONES DE PRIVACIDAD Y SEGURIDAD DE MICROSOFT EDGE

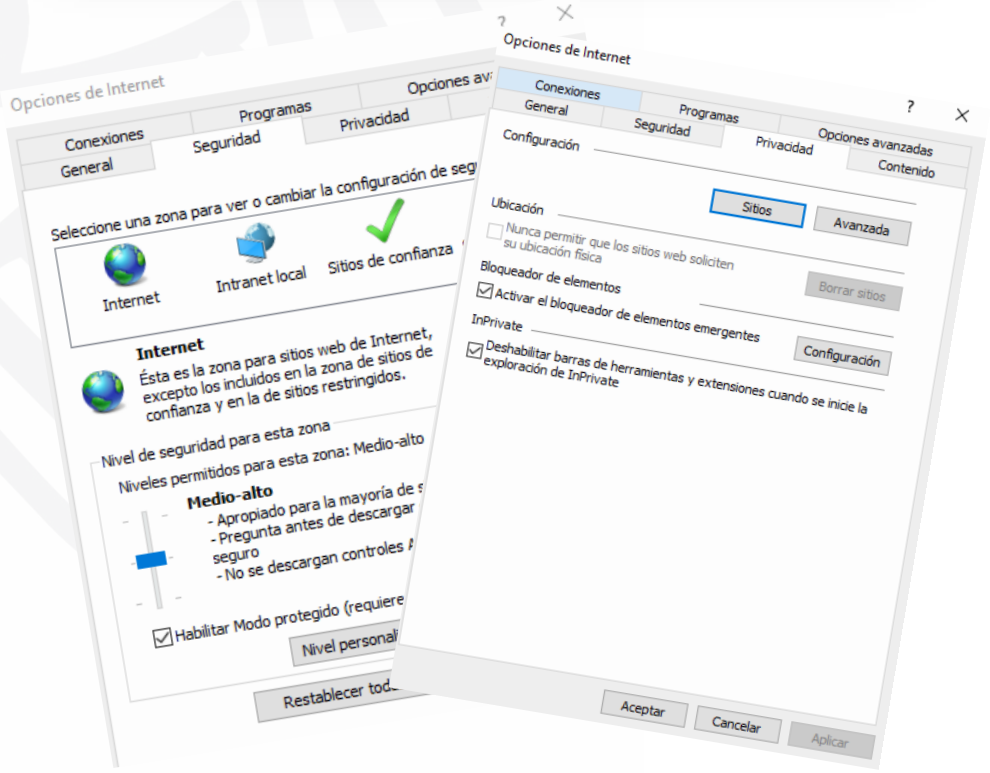
Menú > Configuración > Privacidad, búsqueda y servicios



OPCIONES DE PRIVACIDAD Y SEGURIDAD DE INTERNET EXPLORER

Herramientas> Opciones de Internet > Seguridad

Herramientas> Opciones de Internet > Privacidad



"REVISA LAS OPCIONES DE PRIVACIDAD Y SEGURIDAD DEL NAVEGADOR WEB QUE UTILICES HABITUALMENTE".

MATERIAL COMPLEMENTARIO

- Informe: Seguridad y riesgos de los navegadores web (CCN). Consulta este enlace.
- Guía: Privacidad y Seguridad en Internet (AEPD, INCIBE, OSI). Consulta este enlace.
- Nota Técnica: Medidas para minimizar el seguimiento en internet (AEPD). Consulta este enlace.
- Infografía: Medidas para minimizar el seguimiento en internet (AEPD). Consulta este enlace.
- Blog: Navegación privada para ti y para tu empresa. Parte I (INCIBE). Consulta este enlace.
- Blog: Navegación privada para ti y para tu empresa. Parte II (INCIBE). Consulta este enlace.
- Blog: Riesgos en el uso de extensiones para los navegadores y medidas de seguridad (INCIBE). Consulta este enlace.
- Blog: Navegadores (OSI). Consulta este enlace.
- Blog: Borrando el rastro que dejas al usar el navegador (OSI). Consulta este enlace.

NOTICIAS

- **Entra en vigor el Real Decreto-ley 24/2021, de 2 de noviembre, que transpone directivas de la Unión Europea en determinadas materias como la relativa a los datos abiertos y la reutilización de la información del sector público.** El Libro tercero del incorpora al ordenamiento jurídico español las novedades de la Directiva (UE) 2019/1024 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, relativa a los datos abiertos y la reutilización de la información del sector público. Consulta la norma en este enlace.

- **La AEPD nos habla en su Blog de los recursos para tratar de evitar la publicidad no deseada.** El correo postal, el buzoneo, las llamadas al teléfono fijo o la venta puerta a puerta han sido sustituidas en su gran mayoría por correos electrónicos, mensajes de texto y las especialmente molestas llamadas al teléfono móvil. Diferente normativa, incluida la relacionada con la protección de datos, nos protege de determinadas prácticas comerciales online y offline, pero existen ciertos hábitos o acciones preventivas que podemos llevar a cabo para tratar de evitar la molesta publicidad no deseada o spam. Consulta el Blog en este enlace.

- **La AEPD sanciona a la Consejería de Educación del Principado de Asturias por no utilizar protocolo seguro en su web y por incorporar un apartado de "Trabaja con nosotros" sin dar cumplimiento a la Ley de Servicios de la Sociedad de la Información.** En el procedimiento instruido por la AEPD a la Consejería de Educación del Principado de Asturias, titular y responsable de la página web en cuestión, se sanciona a la citada Consejería por entender que la página no es segura, pues utiliza el protocolo http://; así como por considerar que no cumple con la Ley de Servicios de la Sociedad de la Información, al considerar a la misma "prestador de servicios de la sociedad de la información", pues a través de esta web se gestionaba la bolsa de trabajo del Instituto, posibilitando a los usuarios enviar sus datos personales y su currículum vitae directamente al centro educativo. Consulta la Resolución en este enlace.