Recomendaciones para el uso adecuado de los sistemas judiciales desde fuera de las instalaciones del poder judicial

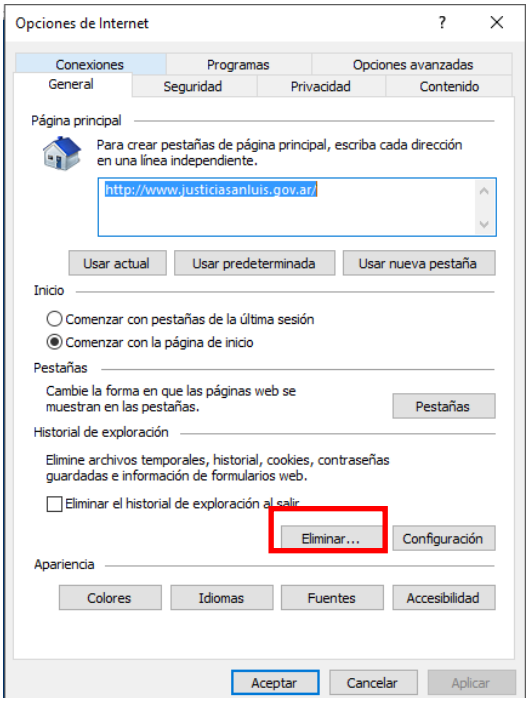
Navegue por internet de forma consciente y segura

Siempre es recomendable navegar por páginas web seguras y de confianza. Para diferenciarlas del resto, identifique si dichas páginas tienen algún sello o certificado que garanticen su calidad y fiabilidad. Las páginas que tienen seguridad en su acceso se pueden identificar de las siguientes dos maneras:

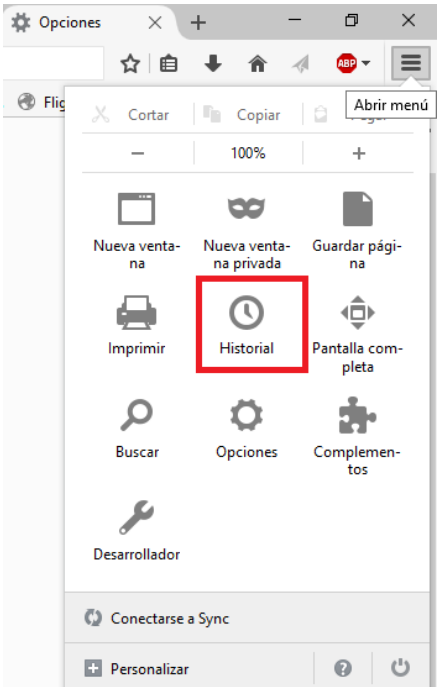
- La dirección de la página debe comenzar con el prefijo https:// en lugar de http://.
- En la barra del navegador debe aparecer el icono del candado cerrado Seguro. Haciendo click en este icono se puede acceder al certificado digital que confirma la autenticidad de la página.

Es conveniente realizar un mantenimiento del navegador periódicamente, eliminando al menos los archivos temporales, historial, datos de formularios y cookies.

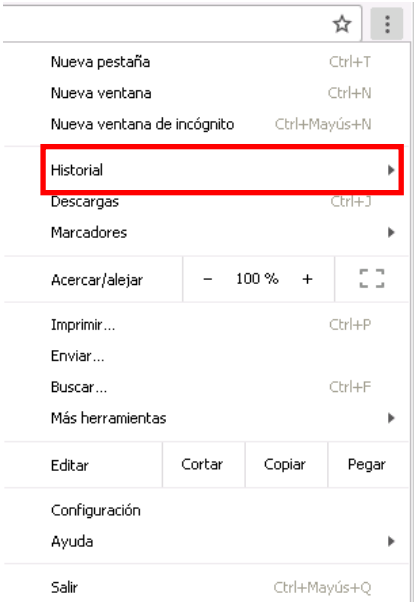
Internet Explorer

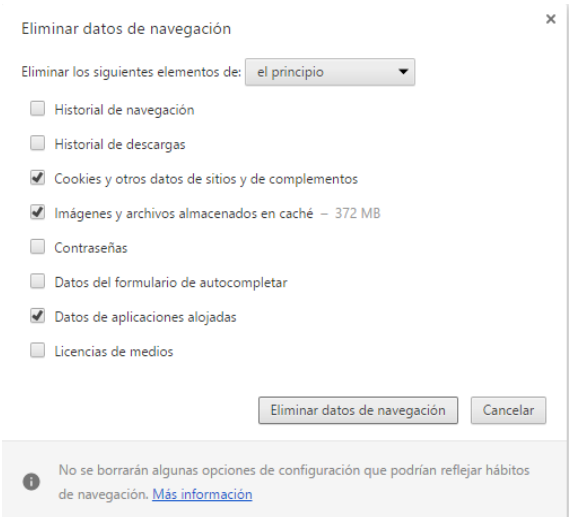


Mozilla Firefox



Chrome





Evite navegar por páginas dudosas y responder los carteles de seguridad o de advertencia que les aparece al navegar en sitios o páginas desconocidas. Siempre lea el mensaje y ante la mínima duda, evite hacer click alguno en el cartel y cierre el navegador o la/s pestaña/s del mismo afectadas.
Extreme estas medidas de precaución al realizar compras online, acceder a su home Banking o enviar información confidencial a través de internet. Siempre es recomendable consultar con alguna persona con conocimiento informático.

Sea cauto con las redes inalámbricas públicas o externas

Evite conectarse a redes inalámbricas "Públicas o Abiertas" desde equipos o dispositivos que tengan información confidencial o relevante.
Si nos conectamos a cualquier red inalámbrica pública, todo lo que accedemos se puede ver comprometido o ser conocido por la persona propietaria del servicio o incluso por otras personas conectadas en la misma red.

Proteja el acceso a sus dispositivos

Siempre es recomendable utilizar contraseñas o algún método de autenticación similar para restringir el acceso a los dispositivos para evitar que otras personas accedan al mismo.
Para el caso de las PC/Notebooks, siempre que se ausente del equipo, bloquee la terminal o sesión de trabajo. En Windows, el atajo de teclado para lograr esto rápidamente consiste en teclear en simultáneo “WIN + L”, o sea, la tecla de Windows junto con la tecla L a la vez.

Cambie sus contraseñas periódicamente

Siempre es recomendable cambiar periódicamente las contraseñas al igual que las medidas de seguridad para recuperarlas. El mecanismo de recuperación de las contraseñas es tan importante como la contraseña misma. No se deben usar frases o preguntas de seguridad con respuestas predecibles o cuentas alternativas de recuperación con contraseñas fáciles, ya que si la cuenta de recuperación se ve comprometida, se rompe la seguridad de la cuenta principal.
Todas las contraseñas que utilices deben ser diferentes para evitar que la vulneración de una de ellas tenga como consecuencia que todas las cuentas se vean comprometidas.
Es fundamental no revelar las contraseñas a otras personas, los vínculos fácilmente se pueden romper y esto lleva a poner en riesgo su información confidencial.

Se precavido con los e-mails recibidos en tu cuenta de correo

Siempre desconfía de los archivos que te envían por más que vengan de un remitente conocido. Siempre es conveniente consultar si no se estaba esperando puntualmente un correo recibido con adjuntos.
Tampoco es aconsejable responder correos que provienen de un remitente sospechoso o desconocido, ni mucho menos abrir o descargar sus adjuntos.

Mantén actualizados el sistema operativo y los programas de tus dispositivos

Es importante trabajar en equipos con sistemas operativos modernos y programas actualizados, debido a que los mismos poseen mejoras y actualizaciones constantes en seguridad. En muchos casos, los sistemas operativos viejos dejan de tener soporte y mantenimiento de seguridad (por ejemplo, windows XP).
No es recomendable instalar programas de fuentes desconocidas.
Use programas antivirus y/o de protección anti-malware y verifique que el Firewall se encuentre activado.
Es recomendable que todas estas tareas las revise su técnico informático de confianza.

Realice copias de resguardo de la información que considere crítica

Para evitar pérdidas de información es conveniente realizar periódicamente el/los resguardos. Cada 2 o 3 meses sería lo ideal.
Siempre realice copias de seguridad en un medio diferente a donde tiene los datos alojados, por ej: realizando el resguardo en DVDs o un disco portátil externo.
También se podría optar de guardar el resguardo usando algún servicio de almacenamiento en la nube (drive, dropbox, icloud, etc), aquí es importante mencionar que usando estos servicios se pierde el control del medio donde se está guardando el backup y no se puede garantizar la confidencialidad de los datos, (al considerar esta opción tener en cuenta la sensibilidad o criticidad de lo que queremos resguardar).
Es importante mantener la copia de seguridad en un lugar distinto al principal para evitar ante cualquier siniestro la pérdida en simultáneo. Además, es recomendable que el resguardo no esté conectado u online (caso de un portátil) ya que si se infecta el equipo con malware, se podría ver afectado el resguardo también.

Educa a quienes comparten el ordenador contigo

Todos los usuarios de un mismo equipo deben tomar las mismas precauciones de seguridad. De nada sirve que uno sea consciente de los riesgos al usar la computadora y la otra persona no. Es conveniente educar al compañero en cuanto a consejos de

seguridad y precauciones ya que el descuido de uno puede comprometer la seguridad de los datos de todos.