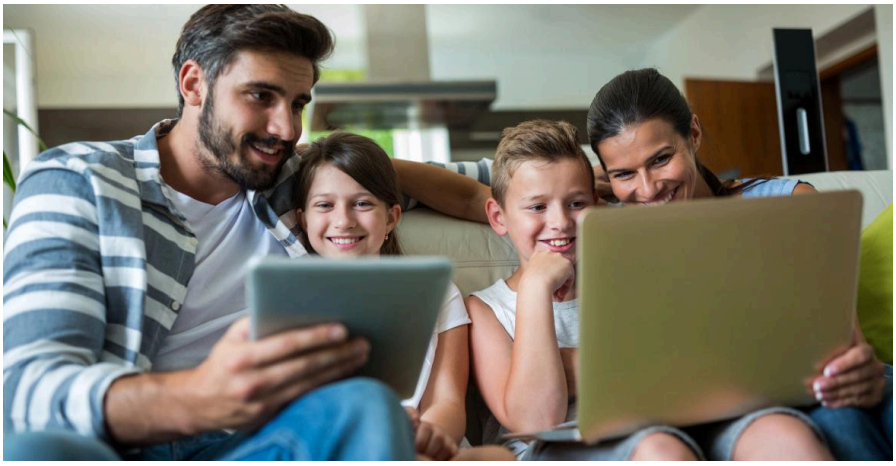
Configuraciones seguras



Introducción

Es fundamental mantener la privacidad, seguridad y bienestar de los/as menores mientras hacen uso de dispositivos con conexión para navegar por Internet. Esta necesidad surge no solo del aumento del uso de los dispositivos, sino también de la constante evolución de los riesgos y amenazas que van apareciendo en el entorno digital.

Para asegurarnos de que los/as menores hacen una navegación segura, es imprescindible tomar las medidas de seguridad necesarias y fomentar hábitos saludables, tanto para el entorno familiar como en el entorno escolar. Además, es necesario actualizar regularmente estas medidas para adaptarse a los posibles cambios en los dispositivos.

La importancia de las configuraciones seguras en la mediación parental

Los padres, madres y tutores legales tienen un papel muy importante a la hora de preparar, tanto a los/as menores antes de empezar a usar los dispositivos, como a estos mismos, y asegurarse así de que hacen un uso seguro y responsable de ellos. Los adultos del entorno familiar de los/as menores pueden ayudar estableciendo límites de tiempo delante de las pantallas, comprobando la seguridad de las aplicaciones que utilizan sus hijos/as, controlando el acceso a webs de contenido inadecuado e, incluso, supervisando su actividad en línea.

Para todo ello, es necesario que el adulto sea consciente de las diferentes opciones de configuración disponibles en los dispositivos y aplicaciones o plataformas que los/as menores utilizan.

En situación

Mario tiene 14 años y utiliza a diario su tableta mientas espera el transporte escolar, hasta que un día olvida el dispositivo en la parada. Es en el trayecto de vuelta cuando se da cuenta de que no lo tiene.

En ese momento lamentó no tener un patrón de desbloqueo configurado en su tableta. Cualquier persona que la haya encontrado, simplemente con deslizar hacia arriba en la pantalla, puede acceder a todo el contenido y aplicaciones que tiene instaladas. Sólo le queda confiar en que su dispositivo haya caído en buenas manos.

¿A qué riesgos se enfrentan si no protegen sus dispositivos?

Cualquiera de nuestros dispositivos (conectados a Internet), o cuentas en redes sociales u otros servicios online pueden poner en riesgo nuestra seguridad, especialmente si no los protegemos de la manera adecuada:

Virus, también llamados malware. Pueden afectarnos de diversas maneras:

- **Daños en el sistema** y sus aplicaciones. Pueden cambiar la configuración del sistema (por ejemplo cambiar la página de inicio del navegador, redirigirnos a páginas maliciosas o fraudulentas en lugar de las oficiales, ofrecernos publicidad) e instalar aplicaciones maliciosas (por ejemplo para ver nuestras contraseñas, secuestrar e inutilizar el dispositivo a cambio de un rescate, utilizar nuestro dispositivo para dañar a otras personas y organizaciones).
- **Daños a nuestra información**. Pueden impedirnos acceder a nuestros documentos, fotos, vídeos, etc. (por ejemplo borrándolos, cifrándolos a cambio de un rescate, estropeándolos al añadir o borrar alguna parte).
- **Pérdidas económicas**. Ayudando a que caigamos, sin darnos cuenta, en páginas web maliciosas (por ejemplo suplantando nuestras redes sociales, bancos y tiendas online), pidiéndonos dinero a cambio de un "servicio" (por ejemplo devolvernos el control del dispositivo, instalarnos un falso antivirus).
- Y también "acceso indebido a información privada" como se detalla a continuación...

Personas que acceden indebidamente a nuestra información privada.

- Daños a la privacidad e intimidad. El mero conocimiento de nuestra información por parte de otra persona sin desearlo. Además se puede agravar si esta información se difunde a otras personas o si se trata de mensajes o imágenes de carácter íntimo.
- Daños en la imagen y reputación online. Si alguien accede a nuestra información privada, y difunde sin nuestro permiso una parte de ella que nos puede resultar perjudicial (por ejemplo imágenes íntimas). También se puede producir por la publicación de mensajes inapropiados, tanto en nuestras propias cuentas de redes sociales como en perfiles falsos que se hacen pasar por nosotros (ridiculizándonos, dañando en nuestro nombre a otras personas).
- Ciberbullying.
- **Grooming, extorsión y chantaje**. Si personas malintencionadas consiguen mensajes e imágenes íntimos, pueden chantajearles y extorsionarles tanto económicamente, como con fines sexuales (para conseguir más imágenes y vídeos, o para abusar sexualmente de ellos).

Recomendaciones para configuraciones seguras

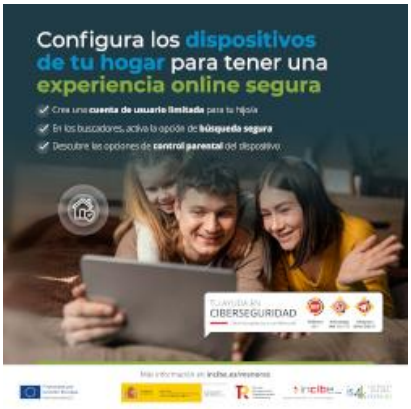
A continuación, compartimos una serie de recomendaciones de seguridad para proteger la información almacenada en los dispositivos y fortalecer su privacidad:

- **Creación de contraseñas seguras y robustas.** Para ello hay que crear una combinación de letras, mayúsculas y minúsculas, números, signos y caracteres. Además, hay que concienciar a los/as menores sobre la importancia de no compartir sus contraseñas con sus amigos ni apuntarlas en un papel para recordarlas, para ello se puede utilizar un gestor de contraseñas.

  Por otro lado, también es conveniente instalar el doble factor de autentificación para añadir una capa extra de seguridad.

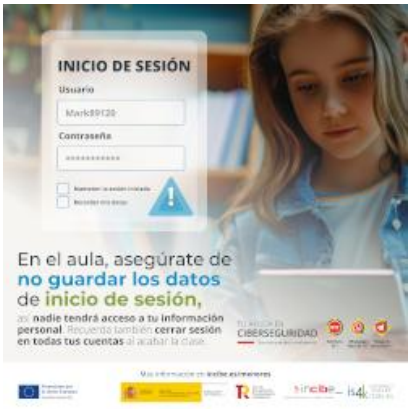
- **Métodos de recuperación de cuenta o contraseña.** En caso de pérdida de la cuenta del/la menor, los métodos de recuperación deben estar bajo el control de las personas que están al cuidado de los/as menores, como son sus padres, madres o tutores legales.
- **Desbloqueo seguro.** Hay diferentes opciones, como el patrón de desbloqueo, la biometría o el uso de una contraseña, para el acceso a los diferentes dispositivos que usan los menores. Puedes ver aquí los patrones de bloqueo más comunes.
- **Realización de copias de seguridad.** Realizarlas, a través de las opciones de los diferentes sistemas operativos de los dispositivos (Android, Windows e iOS), para evitar la pérdida de información o contenido almacenado.

- **Opciones de seguridad.** Donde hay que configurar las opciones adicionales de seguridad que existen en las aplicaciones que utilizan los/as menores, como son las redes sociales, los videojuegos e incluso las plataformas de contenido para garantizar una navegación segura.
- **Opciones de seguridad adicional para dispositivos móviles.** Por ejemplo los servicios de búsquedas de dispositivos como: 'Find My Device' de Google y 'Find my iPhone ' de IOS, que puedes encontrar en el catálogo de herramientas. Así como las aplicaciones y opciones de control parental que faciliten la mediación en el uso de los dispositivos.
- **Instalación de aplicaciones.** Hacerlo siempre desde tiendas oficiales o usar un analizador de URL en el caso de que sea un enlace que desconocemos.
- **Activar alertas de inicio de sesión** para detectar posibles accesos no autorizados.
- **Activar las actualizaciones automáticas.** Actualizar el sistema, las aplicaciones y el antivirus para mejorar la protección del dispositivo.
- Para proteger la información sensible hacer uso de un **programa de cifrado.**
- **Conexión a redes.** Si el dispositivo se conecta a Internet, asegúrate de conectarlo a una red segura y confiable. Si es posible, utiliza una conexión Wi-Fi protegida por contraseña y evita redes públicas no seguras.



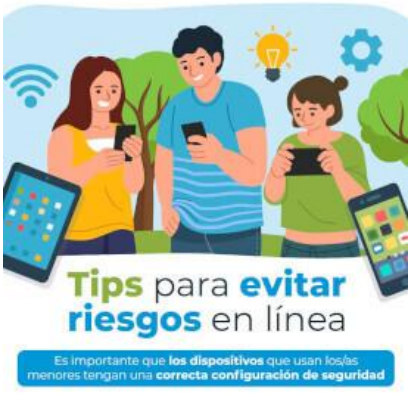
Dispositivos en el hogar (Visual)

Buenas prácticas para un uso seguro de los dispositivos del hogar (Blog)



Dispositivos en el aula (Visual)

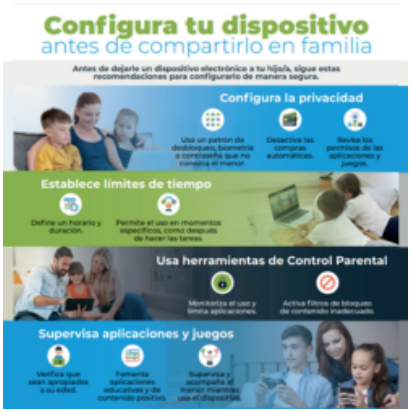
Fomenta las buenas prácticas digitales en el aula (Blog)



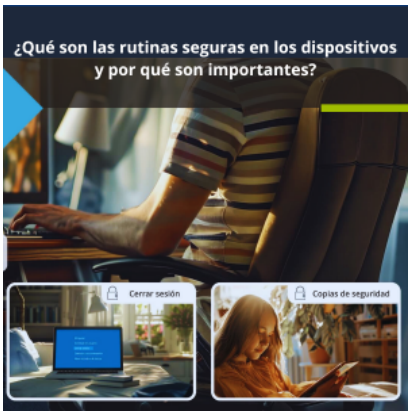
Tips para evitar riesgos en línea (Infografía)

Cámaras en dispositivos: seguridad y privacidad (Blog)

Protege tus trabajos de clase, ¡haz copias de seguridad! (Visual)



Configura tu dispositivo antes de compartirlo en familia (Infografía)



¿Qué son las rutinas seguras en los dispositivos y por qué son importantes? (Vídeo)

Reacción

Si sospechamos de un virus. El dispositivo se comporta de forma extraña, va muy lento, carga páginas y publicidad que no deseamos, el sistema se cuelga, no arranca bien. → Analízalo con tu **antivirus** y/o un antivirus online. Si no es capaz de resolverlo automáticamente, pide ayuda a un profesional.

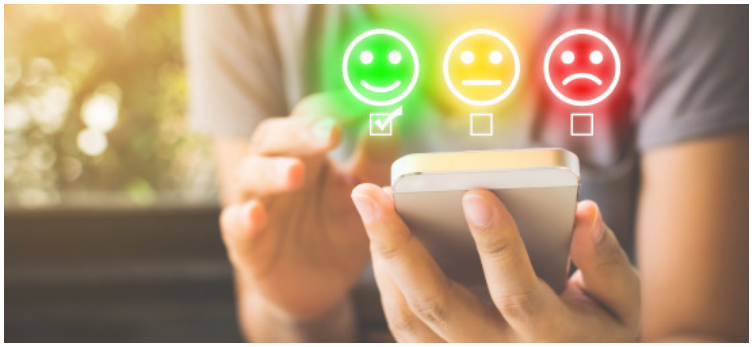
Si hemos perdido información. → Recupera los datos de la **copia de seguridad**. Si te piden dinero a cambio, no cedas al chantaje, no pagues un rescate y contacta con los cuerpos policiales.

Si nos han engañado para acceder a páginas maliciosas que parecían ser las de nuestras redes sociales, bancos o tiendas online. → C**ontacta con la entidad** para alertarla, bloquear los posibles pagos, solicitar la devolución de lo robado. **Cambia tus contraseñas**, tanto en dichas webs, como en el resto (especialmente si son contraseñas similares).

Si alguien comparte nuestros mensajes o imágenes privadas. Se hace pasar por nosotros en redes sociales, publica en nuestro nombre. Nos amenaza o chantajea por Internet. → **Pídele que borre** los mensajes y te devuelva la cuenta. **Repórtalo** en la red social para que los eliminen, te devuelvan el acceso a la cuenta y le bloqueen. **Cambia tus contraseñas** de acceso a las redes sociales y al resto de servicios. Guarda **capturas de pantalla** como evidencia. **Denuncia** en los cuerpos de seguridad y/o fiscalía de menores.

Si no lo tienes claro, tu problema es distinto, o simplemente no sabes por dónde empezar. → Consulta nuestra **línea de ayuda**.

¿Tienes dudas o necesitas ayuda de manera más personalizada en relación con el uso seguro y responsable de los menores en Internet? Contacta con nosotros en la Línea de Ayuda en Ciberseguridad de INCIBE, 017. Es un servicio gratuito y confidencial.



Ayúdanos a mejorar

Tu opinión es muy importante para nosotros.

Contenido realizado en el marco de los fondos del Plan de Recuperación, Transformación y Resiliencia del Gobierno de España, financiado por la Unión Europea (Next Generation).