

MANUAL DE CIBERSEGURIDAD

Conectados y Seguros



Elaborado por Equipo @ Córdoba



ÍNDICE

- 1. INTRODUCCIÓN A LA CIBERSEGURIDAD.**
- 2. CONCEPTOS CLAVE DE CIBERSEGURIDAD.**
- 3. PRINCIPALES AMENAZAS Y RIESGOS ONLINE.**
- 4. SEGURIDAD EN INTERNET MENORES (6 A 12 AÑOS).**
- 5. BUENAS PRÁCTICAS DE SEGURIDAD.**
 - 5.1 Contraseñas Seguras
 - 5.2 No compartir información personal
 - 5.3 Utiliza Herramientas de Seguridad
 - 5.4 Controla tu tiempo
 - 5.5 Estrategias contra la TECNOADICCIÓN
 - 5.6 Descarga Aplicaciones y juegos confiables
- 6. BUEN USO DE LOS DISPOSITIVOS TIC.**
 - 6.1 El Móvil y Tú: 10 TIPS para usarlo responsablemente
- 7. MEDIACIÓN-CONTROL PARENTAL.**
 - 7.1 Estrategias de la mediación parental
 - 7.2 Métodos de control parental
 - 7.3 Herramientas de control parental
- 8. USO RESPONSABLE DE LAS REDES SOCIALES.**
 - 8.1 Riesgos y amenazas en las RR.SS.
 - 8.2 Uso de las RR.SS. con responsabilidad
- 9. EDUCACIÓN Y CIUDADANÍA DIGITAL.**
 - 9.1 Métodos para fomentar la Educación Digital
 - 9.2 Herramientas de uso para Educación Digital
 - 9.3 ¿Cómo nos adaptamos según la edad?
 - 9.4 Ciudadanía e Identidad Digital
 - 9.5 Construye una Identidad Positiva
- 10. RESPUESTA ANTE UN INCIDENTE.**
 - 10.1 ¿Y si Deseo presentar una Denuncia?
 - 10.2 ¿Dónde y de qué forma Denunciar?
 - 10.3 Líneas de Ayuda



1

INTRODUCCIÓN A LA CIBERSEGURIDAD

En la era digital actual, donde gran parte de nuestras actividades diarias se desarrollan Online, la ciberseguridad se ha vuelto fundamental para proteger nuestra información y garantizar una navegación segura. Desde la comunicación con amigos y familiares hasta el aprendizaje en línea y la gestión de datos personales, dependemos de dispositivos y plataformas digitales para realizar tareas importantes. Sin embargo, el mundo digital presenta riesgos y amenazas que debemos conocer para evitarlos.

Este manual está diseñado para padres, madres, profesionales de la enseñanza y jóvenes menores en edad escolar, y tiene como objetivo principal tener un conocimiento básico de los riesgos y amenazas que pueden surgir por el uso de Internet, así como sensibilizar y educar sobre prácticas seguras en el entorno digital.

La **Ciberseguridad**, abarca un conjunto de técnicas, acciones, prácticas y conocimientos que permiten proteger nuestros dispositivos (ordenadores, móviles, tablets, etc), nuestra información y nuestra privacidad en Internet. (TIC).

La **ciberseguridad** es una responsabilidad compartida. Vivimos en un mundo cada vez más **conectado**, por lo que es fundamental que aprendamos a mantenernos **seguros** mientras navegamos por la red.

Al trabajar juntos para comprender y aplicar estas prácticas, podremos construir un espacio online más positivo y respetuoso para todos.

2

CONCEPTOS CLAVE DE CIBERSEGURIDAD

Para comprender mejor el mundo de la ciberseguridad, es importante familiarizarse con algunos términos clave. Este glosario ofrece definiciones esenciales que ayudarán a adultos y jóvenes alumnos a navegar de manera más segura en el entorno digital.

Qué son las TIC

Conjunto de herramientas que permiten el procesamiento, almacenamiento y transmisión de información: Imágenes, texto, audio y video. (Teléfonos móviles, PC, Tablet, RR.SS, App, etc).

Las TIC han experimentado un crecimiento exponencial en las últimas décadas, transformando profundamente la forma en que interactuamos, aprendemos y nos comunicamos en la sociedad moderna.





2.1 Definiciones básicas de ciberseguridad

- **Antivirus:** Software que detecta y elimina malware de los dispositivos.
- **Autenticación de Dos Factores (2FA):** Método de seguridad que requiere dos verificaciones para acceder a una cuenta.
- **Ciberacoso:** Acoso o intimidación a través de medios digitales.
- **Contraseña Segura:** Clave que combina letras, números y símbolos para proteger cuentas.
- **Copia de Seguridad (Backup):** Proceso de crear copias de datos para prevenir su pérdida.
- **Firewall:** Herramienta que filtra el tráfico de red y bloquea accesos no autorizados.
- **Fake news:** Información falsa o engañosa difundida como noticia, diseñada para desinformar o manipular al público.
- **Ingeniería Social:** Manipulación psicológica para obtener información o acceder a sistemas.
- **Malware:** Software malicioso diseñado para dañar o infiltrarse en sistemas.
- **Navegación Segura:** Prácticas que ayudan a proteger la información al navegar en internet.
- **Navegador Web:** Es un programa que permite ver la información que contiene una página web.
- **Phishing:** Técnica de engaño para robar información personal a través de correos o sitios falsos.
- **Ransomware:** Malware que bloquea el acceso a datos y exige un rescate.
- **Redes Seguras:** Conexiones a internet que están protegidas contra accesos no autorizados.
- **VPN (Red Privada Virtual):** Herramienta que proporciona una conexión segura y encriptada a internet.
- **Wi-Fi:** Tecnología de redes inalámbricas que permite a los dispositivos electrónicos conectarse entre sí.

3

PRINCIPALES AMENAZAS Y RIESGOS ONLINE

A medida que usamos Internet, también nos enfrentamos a diversos peligros y amenazas que pueden afectar a nuestra seguridad y privacidad. Esta sección aborda las amenazas más comunes que pueden afectar a nuestros jóvenes y menores, siendo crucial conocerlas.

Posteriormente, en las siguientes secciones de este manual, desarrollaremos y veremos que medidas podremos adoptar para protegernos contra ellas.



CYBERBULLYING

También conocido como “acoso virtual” es el uso de medios digitales para acosar, amenazar o difundir información personal, dañina o falsa sobre una o varias personas.

Cómo opera: Puede manifestarse en forma de mensajes ofensivos, publicaciones difamatorias, o divulgación de información sensible.

Ejemplo: Un estudiante recibe mensajes abusivos en RR. SS., lo que afecta a su bienestar emocional.

Medidas preventivas: Configurar las opciones de privacidad, no responder a provocaciones y bloquear a personas acosadoras. En casos graves, reportar y solicitar ayuda.





GROOMING

Es una práctica de acoso en línea en la que un adulto establece una relación de confianza con un menor para manipularlo o abusar de él emocional o sexualmente.

Cómo opera: Un adulto se hace pasar por un joven en RR.SS. para ganar su confianza.

Ejemplo: Un joven recibe mensajes en su perfil de Facebook con halagos para ganarse la confianza del menor, posteriormente solicita información personal e íntima.

Medidas preventivas: Utiliza perfiles privados en las RR.SS. Configura las opciones de privacidad. No respondas a personas desconocidas. NO envíes fotografías tuyas que te puedan comprometer.



PHISHING

Es una técnica de engaño mediante la cual un atacante se hace pasar por una entidad o persona confiable para obtener información sensible.

Cómo opera: Usualmente, el usuario recibe un correo electrónico, mensaje de texto o enlace que lo redirige a un sitio web falso, diseñado para parecer legítimo.

Ejemplo: Un usuario recibe un correo supuestamente de su banco solicitándole que actualice su información de cuenta; al hacer clic, es redirigido a un sitio web falso donde ingresa sus datos.

Medidas preventivas: No hacer clic en enlaces sospechosos, verificar el remitente de los correos y acceder a sitios bancarios escribiendo la URL manualmente.



ACCESO A CONTENIDO INAPROPIADO

Visualización en páginas Web y RR.SS. de publicaciones con contenido violento, pornográfico o relacionado con el odio.

Cómo opera: Los jóvenes de forma voluntaria o involuntaria acceden a páginas web a través de enlaces de la red.

Ejemplo: Un adolescente descarga una App de videos. Al explorar el contenido, es redirigido a enlaces externos con material violento.

Medidas preventivas: Utilizar filtros de contenido y control parental en dispositivos y redes. Supervisar el tiempo de uso.



ADICCIÓN A LAS TIC

Es el uso excesivo y compulsivo de dispositivos digitales y plataformas online, como Teléfonos, RR.SS., videojuegos e Internet en general.

Cómo opera: Debido al estímulo constante de notificaciones y recompensas virtuales, se logra un gran impacto en su bienestar emocional.

Ejemplo: Un joven estudiante se pasa varias horas al día en RR.SS., descuidando sus estudios y actividades físicas, sintiéndose ansioso si no tiene su dispositivo.

Medidas preventivas: Configurar límites de tiempo en App y establecer horarios sin tecnología. Fomentar las actividades físicas y sin pantallas.



SUPLANTACIÓN DE IDENTIDAD

Consiste en la creación de perfiles o sitios falsos para hacerse pasar por otra persona con el fin de engañar a terceros y obtener información o beneficios.

Cómo opera: Los delincuentes crean perfiles idénticos en redes sociales o correos electrónicos similares para confundir a amigos o conocidos y obtener información o dinero.

Ejemplo: Un estafador crea un perfil falso en redes sociales haciéndose pasar por un amigo y pide dinero prestado a otros contactos.

Medidas preventivas: Ser cauteloso con solicitudes inusuales, verificar identidades y reportar cuentas falsas en redes sociales.



FAKE NEWS

Noticias falsas, bulos, difusión de información falsa o inexacta, que puede manipular a los usuarios o generar pánico. difundido a través de noticias en prensa, radio, televisión y RR.SS.

Cómo opera: Puede propagarse por redes sociales, medios de comunicación o mensajes de grupo, apelando a emociones o prejuicios.

Ejemplo: Un mensaje viral asegura que un producto común causa enfermedades graves, generando preocupación sin fundamentos científicos.

Medidas preventivas: Verificar fuentes de información, no compartir contenido dudoso y usar sitios de verificación de hechos.



FRAUDE-COMPRAS ONLINE

Estafas en las que los ciberdelincuentes engañan para obtener dinero o información personal mediante web falsas u ofertas engañosas en páginas de comercio digital.

Cómo opera: Usuarios son engañados en web o anuncios falsos que simulan tiendas legítimas, donde se pagan productos que luego nunca se reciben.

Ejemplo: Usuario observa un producto de marca comercial muy reconocida y el cual se encuentra a un precio muy bajo. Al ingresar sus datos y realizar el pago, no recibe el artículo ofertado.

Medidas preventivas: Verificar las webs con el candado de seguridad (<https://>) y leyendo reseñas. Usar métodos de pago seguros, como tarjetas virtuales o servicios de pago que ofrezcan protección al comprador.

RECUERDA QUE...



INTERNET es un mundo lleno de oportunidades y recursos maravillosos, pero también conlleva ciertos riesgos.

Navegar de forma segura implica estar conscientes de las amenazas y tomar medidas preventivas para protegernos y disfrutar plenamente de sus beneficios.

4

SEGURIDAD EN INTERNET MENORES DE 6 A 12 AÑOS

A medida que los niños y niñas comienzan a explorar el mundo digital, es crucial guiarlos para que desarrollen hábitos seguros y responsables.

Desde elegir sitios adecuados, hasta entender la importancia de la privacidad, estas prácticas y recomendaciones están diseñadas para que padres, madres y educadores ayuden a los menores a navegar de forma segura y así proteger a los más pequeños mientras disfrutan y aprenden del entorno digital.



• Navegación Supervisada



Acompaña a los niños mientras usan Internet, especialmente si están visitando nuevos sitios o aplicaciones.

Explícale que es importante que te muestre cualquier cosa en línea que le parezca extraña e incómoda.

• Elegir Sitios y Apps Adecuadas para su Edad



Selecciona web, juegos y App diseñadas para menores, que cuenten con certificaciones de seguridad y privacidad. Existen multitud de ellas con buena reputación y clasificadas por edades.

• Configurar el Control Parental



Activa el control parental en dispositivos y redes sociales para limitar el acceso a contenido inadecuado y controlar el tiempo de uso.

Revisalo regularmente para ajustar configuraciones según la edad y necesidades del niño.

• No Compartir Información Personal



Enséñales a no compartir datos como nombre completo, dirección, teléfono o escuela en redes sociales, chats o juegos en línea.

Recuérdales que, si alguien les pide información personal, deben consultar siempre contigo o con un adulto de confianza.

• Crear Contraseñas Seguras y Mantenerlas en Privado



Si los niños usan cuentas online, ayúdales a crear contraseñas seguras y explícales que no deben compartirlas con nadie, excepto contigo. Usa contraseñas fáciles de recordar pero difíciles de adivinar, combinando letras, números y símbolos.

• Identificar y Evitar Publicidad Engañosa



Enséñales a reconocer anuncios y a evitar hacer clic en enlaces de ventanas emergentes o premios que aparecen mientras navegan.

Explícales que muchos anuncios intentan que descarguen cosas que pueden ser dañinas.

• Ser Amable y Respetuoso en Línea



Promueve una conducta respetuosa y amable cuando interactúen con otros, explicándoles la importancia de tratar bien a los demás.

Usa ejemplos para explicar qué hacer si alguien es irrespetuoso o los hace sentir incómodos.

• Reportar Situaciones de Acoso o Contenido Inapropiado



Enséñales a hablar contigo o con un adulto de confianza si encuentran algo en Internet que les incomode o que no entiendan.

Recuérdales que no están solos y que es esencial mostrar las situaciones que le generen malestar.

• Limitar el Tiempo Frente a la Pantalla



Define un límite de tiempo para el uso de dispositivos, equilibrando el tiempo de pantalla con otras actividades saludables como el juego físico y el estudio.

Puedes usar temporizadores o apps para ayudar a los niños a manejar el tiempo frente a la pantalla.

• Actualizaciones y Antivirus



Asegúrate de que los dispositivos y App que los menores usan estén actualizados y cuentan con antivirus para protegerlos de malware.

Activa actualizaciones automáticas y revisa regularmente la seguridad de los dispositivos.



5

BUENAS PRÁCTICAS DE SEGURIDAD

Mantenerse seguro en Internet requiere adoptar hábitos sencillos que protejan nuestra información y privacidad. En esta sección, exploraremos prácticas clave para navegar de manera segura, proteger nuestras cuentas y evitar riesgos comunes online. Siguiendo estos consejos, podemos reducir considerablemente las amenazas y disfrutar de una experiencia digital más segura.





5.1 Contraseñas Seguras

Crear contraseñas seguras es esencial para proteger nuestra información digital. En este punto aprenderás a crear claves fuertes, fáciles de recordar y difíciles de adivinar, que mantendrán tus cuentas seguras frente a accesos no autorizados.

- ✓ **Longitud:** Utiliza contraseñas largas, preferiblemente de al menos 12 caracteres, Incluye letras mayúsculas, minúsculas, números y símbolos especiales en tu contraseña (@, #). Las contraseñas cortas son más fáciles de averiguar por otras personas.
- ✓ **Evita información personal:** No uses datos personales como tu nombre, fecha de nacimiento o palabras fáciles de adivinar.
- ✓ **Distintas contraseñas para distintos servicios:** No uses la misma contraseña para múltiples cuentas.
- ✓ **Autenticación de dos factores (2FA):** Habilita la autenticación de dos factores cuando sea posible, para añadir una capa adicional de seguridad.
- ✓ **Mantén tus contraseñas seguras:** No compartas tus contraseñas con nadie y guárdalas en un lugar seguro, o utiliza una herramienta de gestión de contraseñas para generar y almacenar.
- ✓ **Cambia las contraseñas periódica y regularmente.**



5.2 No compartir información personal

Nunca debemos compartir información personal (Datos bancarios, Dirección, documentos de identidad, datos familiares, etc), esto es fundamental para proteger nuestra privacidad. Estos datos pueden ser utilizados por ciberdelincuentes para suplantar nuestra identidad, cometer fraudes o acosos.

Aquí tienes algunos consejos prácticos:

- ✓ **Revisa tu configuración de privacidad:** Configura tus cuentas para que sólo tus amigos y personas de confianza puedan ver tu perfil y publicaciones.
- ✓ **Cuida el contenido de tus fotos:** No compartas y evita publicar imágenes íntimas e información sensible.
- ✓ **Ignora en RR.SS. solicitudes de desconocidos:** No respondas a mensajes de desconocidos, ni facilites información adicional.
- ✓ **Enseña a los jóvenes menores a identificar riesgos:** Explícales que no deben compartir información familiar, ni siquiera en juegos online.
- ✓ **Usa el doble factor de autenticación:** Esto añade una capa de seguridad, reduciendo el riesgo de acceso. No autorizado.





5.3 Utiliza Herramientas de Seguridad

Proteger nuestra información y dispositivos es clave para una experiencia segura en Internet. Existen diversas herramientas que nos ayudan a fortalecer la seguridad digital. A continuación, te compartimos algunos de los consejos más importantes:

- ✓ **Mantén tus dispositivos y App actualizados:** Las actualizaciones suelen incluir parches de seguridad que protegen contra las últimas amenazas.
- ✓ **Usa un antivirus actualizado:** Instala y mantén actualizado un antivirus en todos tus dispositivos para detectar y eliminar amenazas.
- ✓ **Realiza copias de seguridad periódicas:** Haz copias de tus archivos importantes en un disco externo o en la nube. Esto asegurará que no pierdas la información.
- ✓ **Activa el control parental:** Si hay menores de edad usando dispositivos, estas configuraciones pueden protegerlos de contenido inapropiado.
- ✓ **Utiliza una VPN en redes Wi-Fi públicas:** Conéctate de forma segura a Internet cuando uses redes públicas. Una Red Privada Virtual (VPN) encripta tus datos y protege tu privacidad en redes abiertas.





5.4 Controla tu tiempo

El uso excesivo de la tecnología puede provocar “**TECNOADICCIÓN**”, afectando a nuestra salud y relaciones personales. Controlar el tiempo de uso de los dispositivos digitales es fundamental para mantener un equilibrio saludable. Te presentamos algunas consideraciones y estrategias efectivas que te ayudarán ante un problema de Tecnoadicción.

TECNOADICCIÓN

Comportamiento compulsivo relacionado con el uso excesivo de la tecnología

SÍNTOMAS

Largas horas usando
TIC

Pérdida de interés en
actividades OFFline

Necesidad de uso
prolongado

Aislamiento Social
pérdida de relaciones

Ocultamiento del uso
de las TIC

Negación o minimizar
el uso de TIC

Problemas de
Conducta:
Deterioro del sueño

Descuido
responsabilidades
personales



5.5 Estrategias contra la TECNOADICCIÓN

Frente a un problema de **TECNOADICCIÓN** es importante abordarlo de manera comprensiva y efectiva. Para ayudar a los padres, madres y educadores en esta situación, aquí tienes una serie de recomendaciones:

Establece una comunicación abierta con tu hijo, escucha y no juzgues sus experiencias.

Educa sobre las consecuencias negativas de la Tecnoadicción

Establece límites claros sobre el tiempo y uso de las TIC.

Ofrece a tu hijo alternativas saludables para el tiempo libre.

Sé un modelo positivo, muestra un uso equilibrado y responsable de las TIC.

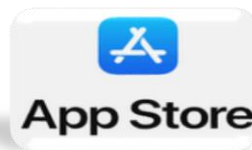


**RECUERDA, SI CREEMOS QUE EL JOVEN
MENOR SUFRE ADICCIÓN:
OFRÉCELE APOYO Y COMPRENSIÓN
BUSCA AYUDA DE UN ESPECIALISTA**

5.6 Descarga Aplicaciones y juegos confiables

Una de las principales fuentes de riesgo en Internet es la descarga de Aplicaciones y juegos desde sitios de poca confianza, ya que pueden incluir malware o virus. Para protegernos a nosotros y a los dispositivos, te recomendamos que:

Realices las descargas de aplicaciones únicamente de tiendas oficiales como **Google Play Store** para Android, **App Store** para IOS o tiendas verificadas de consolas de videojuegos como **Nintendo E-shop**, **PlayStation** y **Xbox**. Estas tiendas pasan por procesos de verificación de seguridad que reducen significativamente el riesgo de malware



Antes de iniciar cualquier descarga verifica la reputación del juego, mira su calificación y reseñas.

Revisa los permisos solicitados (Acceso a contactos, cámara, geolocalización), configura el control parental y mantén siempre que puedas actualizadas todas las aplicaciones.



6

BUEN USO DE LOS DISPOSITIVOS TIC

*Haz un buen uso,
sin abuso y con
responsabilidad*

En la era digital que vivimos, proteger nuestro dispositivo es esencial para resguardar la privacidad y seguridad de nuestra información. A continuación, te mostramos un Decálogo de buenos hábitos de las Tecnologías de la Información y Comunicación (TIC) en las familias.



Protejan la privacidad familiar: No compartan Información de los miembros familiares en RR.SS.



Establecer contraseñas **seguras y únicas**, diferenciadas para cada miembro de la familia en sus dispositivos.



Promover el **respeto y comunicación positiva**. Responsables y amables en las interacciones.



Configuren el **control parental** y los filtros de contenido en los dispositivos de los jóvenes.



Eviten las **descargas de aplicaciones** o los archivos de fuentes desconocidas para reducir riesgos.



Enseñen a **verificar la veracidad** de las noticias e información antes de compartirla.



Establecer **horarios y límites** de uso de las TIC, que promuevan el equilibrio entre diferentes actividades.



Eduquen sobre el **ciberacoso y la seguridad** online, y hablen sobre los riesgos de Internet y como actuar ante un problema.



Realicen **copias de seguridad** (Backup), regularmente de toda la información familiar importante.



Manténganse **informados** sobre seguridad digital. Actualicen sus conocimientos para enfrentarse a los desafíos.

6.1 El Móvil y Tú: 10 TIPS para usarlo responsablemente

Decálogo de buen USO



01
Limita el tiempo en
pantalla y establece
horarios para su uso

02
Protege tu privacidad,
evita compartir fotos
con extraños

03
Se respetuoso con tus
palabras y
publicaciones

04
Apaga el móvil en clase
y en las horas de
descanso

05
No caigas en rumores,
verifica la información
antes de creerla

06
App seguras,
apropiadas para tu
edad. Se selectivo

07
Márcate momentos
libres de móvil. No todo
es digital

08
Comparte con tus
padres, sobre todo lo
que haga sentir mal

09
Deja el móvil en casa.
Aprende a vivir sin el

09
Fomenta las relaciones
personales y habla con
los amigos



Recuerda que:

¡ Los ADULTOS son los primeros que tienen que dar ejemplo !

7

MEDIACIÓN – CONTROL PARENTAL

La **mediación parental** implica un conjunto de estrategias, herramientas y medidas que emplean padres y madres para proteger a los menores en Internet. Supervisando, guiando y apoyando a los jóvenes en el uso de la tecnología.

¿En qué dispositivos puedo configurar el control parental adecuado para mi familia?



ORDENADOR



MÓVIL



TABLET



TELEVISIÓN



CONSOLA

Muchos de los servicios de Internet ofrecen opciones de control parental:

-  REDES SOCIALES
-  JUEGOS EN LÍNEA
-  APLICACIONES
-  PLATAFORMAS DE TELEVISIÓN
-  JUGUETES CONECTADOS





7.1 Estrategias de la mediación parental

El control parental se basa en dos enfoques principales, permitiendo gestionar y supervisar el uso de la tecnología por parte de los jóvenes menores. Pueden ser:

- **Activa:** Basada en el acompañamiento, orientación y supervisión mediante el diálogo familiar.
- **Restictiva:** Estableciendo límites y controles en los dispositivos o servicios.

SUPERVISIÓN ACTIVA

Presta atención a lo que hace mientras está conectado

Dialoga sobre el uso seguro y comportamiento responsable de internet

Elige contenidos apropiados a su edad y madurez

Crea un clima de confianza y respeto mutuo

Mantén el equilibrio en el tiempo de uso de las TIC

SUPERVISIÓN RESTRICTIVA

Conoce y usa las herramientas de control parental

Establece reglas y límites, atendiendo al sentido común y madurez del menor

Prepara un entorno TIC ajustado a la madurez del menor

Bloquea compras no autorizadas y descargas

Pacta para limitar el uso de las TIC

7.2 Métodos de control parental



Son App y configuraciones diseñadas para proteger a los jóvenes menores de las amenazas online.

No sustituyen la supervisión o el acompañamiento, pero pueden ser nuestras aliadas.

Existen diferentes métodos de control parental:



Límites de tiempo en pantalla: Fijan un horario de uso y bloquean las aplicaciones o el dispositivo

Filtros de contenido: Limita el acceso a determinados contenidos inapropiados para su edad.

Supervisión de actividades en línea: Registros de uso y alerta, permiten ver que ha visitado o con quien ha contactado.

Configuración de privacidad y seguridad: Configurar correctamente las opciones o ajustes en los dispositivos y cuentas en línea.



Recuerda que:

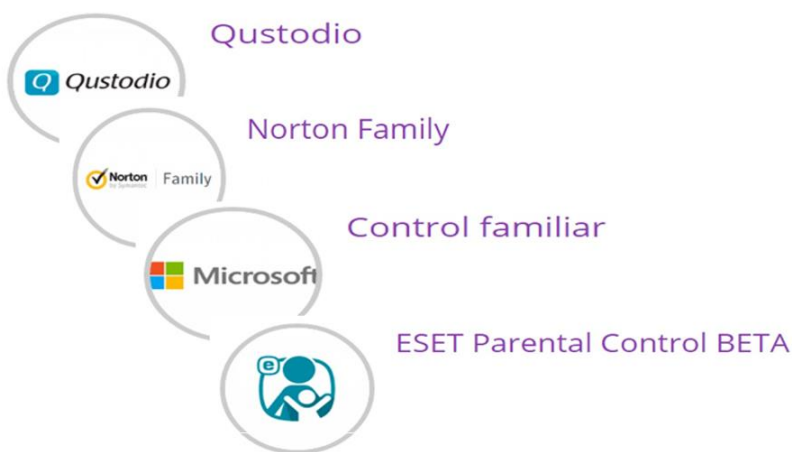
Cada App, juego online o red social posee opciones de configuración que debemos de determinar juntos, para que todos seamos conscientes de los límites de uso.



7.3 Herramientas de control parental

Estas herramientas son aplicaciones, programas o funciones integradas en dispositivos que permiten a los padres y madres supervisar, gestionar y limitar el acceso de los menores y adolescentes al contenido digital. Estas herramientas son esenciales en la era tecnológica para protegerlos de los riesgos en la red.

A continuación, te proponemos el uso de algunas de las aplicaciones más populares y ampliamente utilizadas, las cuales ofrecen multitud de funciones y recursos.



¡RECUERDA...!

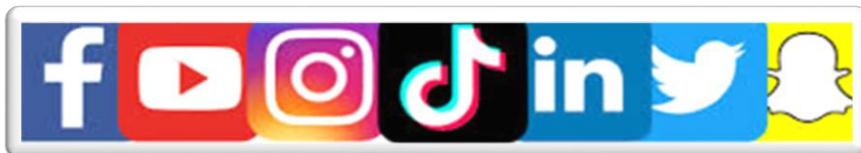
Estas Aplicaciones NO sustituyen la supervisión o el acompañamiento, pero pueden ser nuestras aliadas.

Estas Herramientas están disponibles en los principales Sistemas Operativos Windows, MacOS, Android e IOS, y entre sus principales funciones destacan:



8

USO RESPONSABLE DE LAS REDES SOCIALES



Las RR.SS. son unos servicios Online donde cada usuario/a tiene un perfil con una serie de datos, que le permite comunicarse y compartir información con otras personas.

Son unas poderosas herramientas de comunicación, están en sus móviles, y estos les acompañan en todo momento.

Las RR.SS. son un lugar de encuentro donde los jóvenes pueden interactuar en tiempo real con personas de su misma edad, mediante publicaciones, comentarios o chat en vivo. Comparten multitud de experiencias con fotografías y videos.

Permiten crear vínculos y entablar contactos, así como explorar y expresar su identidad



Los perfiles pueden ser **públicos o privados**.

¡¡ En los **MENORES PERFIL = PRIVADO** ¡¡

Aunque sus publicaciones solo lleguen a sus contactos en privado, estos pueden hacerlas públicas. ¡¡**DESCONFIAR SIEMPRE**¡¡

8.1 Riesgos y amenazas en las RR.SS.

Las RR.SS. ofrecen muchos beneficios, pero también implican riesgos y amenazas, especialmente en términos de privacidad, seguridad y bienestar psicológico, a continuación, explicamos los más habituales.

AL EXPONER INFORMACIÓN PERSONAL

Suplantación de identidad: Otro Usuario puede utilizar sus imágenes y datos para crear un perfil falso y utilizarlo de forma dañina.

Grooming: Un adulto puede hacerse pasar por un menor, para ganar su confianza.

AL UTILIZARLAS DE FORMA INADECUADA

Ciberacoso: Comentarios y publicaciones negativas o humillantes hacia una persona

Uso excesivo: Aparición de síntomas de dependencia física, social y educativa.

AL ACCEDER A CONTENIDOS INAPROPIADOS

Bulos y fraudes: Noticias falsas para crear desinformación o alarma social.

Discursos de odio: Contenidos irrespetuosos generando actitudes violentas.





8.2 Uso de las RR.SS. con responsabilidad

Usar las RR.SS. de forma responsable implica tener en cuenta tanto la seguridad propia como el impacto que nuestras acciones pueden tener en los demás. Aquí te presento una serie de pautas para que ayudes a tus hijos e hijas a utilizarlas de forma responsable.

ELIGE LA RED SOCIAL ADECUADA

Ten en cuenta su edad y madurez
Analiza las características de cada plataforma
Revisa todas las opciones de seguridad de la R.S.

GESTIONA Y CONTROLA LAS AMISTADES

Contacto sólo con personas conocidas
Con ayuda de un adulto identificar solicitudes con riesgo
Se selectivo con las personas que agregas

CREA UNA BUENA IDENTIDAD DIGITAL

Cuidar de la imagen pública del menor, pensar en la repercusión del futuro y construye una Identidad positiva

CREA CONTENIDO POSITIVO

Generar contenidos que transmitan valores e información veraz



EDUCACIÓN Y CIUDADANÍA DIGITAL



La **educación digital** es el proceso de enseñar y aprender sobre el uso seguro, responsable y efectivo de las tecnologías digitales. Involucra el desarrollo de habilidades y conocimientos necesarios para que los jóvenes puedan navegar en el mundo digital con confianza, respetando tanto su privacidad como la de los demás. La educación digital no solo incluye saber cómo

usar herramientas tecnológicas, sino también comprender temas importantes como la seguridad en Internet, la protección de datos personales, el respeto en redes sociales, el manejo de la información y la detección de riesgos online.

Para padres, madres y educadores, la educación digital es fundamental para preparar a los niños, niñas y adolescentes para un mundo digital en constante cambio, ayudándoles a tomar decisiones informadas y a actuar de manera ética en sus actividades en Internet.

Veamos a continuación una serie de métodos que nos ayudarán a fomentar la Educación Digital.





9.1 Métodos para Fomentar la Educación Digital

• Charlas Abiertas y Frecuentes sobre Seguridad en Línea

Crear un ambiente de confianza donde los adolescentes se sientan cómodos para hablar sobre sus experiencias en Internet.

• Uso de Recursos Educativos Digitales

Existen plataformas y herramientas que, explican temas complejos de manera accesible y atractiva para diferentes edades, ayudando a los jóvenes a navegar de forma segura.

• Modelar Buenas Prácticas de Ciberseguridad

Los adultos pueden enseñar con el ejemplo, demostrando comportamientos seguros en línea, como usar contraseñas seguras, verificar fuentes de información y evitar compartir información privada.

• Establecer Reglas Claras de Uso de Dispositivos y Redes Sociales

Acordar pautas específicas sobre el tiempo de pantalla, qué tipo de contenido pueden acceder y con quiénes pueden interactuar en redes.

• Fomentar el Pensamiento Crítico sobre el Contenido Digital

Enseñar a los niños a cuestionar la veracidad de la información que encuentran en Internet. Ayúdalos a reconocer noticias falsas, estafas y perfiles sospechosos para evitar manipulaciones.

• Usar Software de Control Parental como Apoyo

Los programas de control parental ayudan a supervisar el acceso a contenido y proteger a los jóvenes en sus primeras experiencias digitales. Sin embargo, es importante acompañar estas herramientas con una educación que explique el porqué de las restricciones y promueva la autorregulación con el tiempo.



9.2 Herramientas de uso para Educación Digital

Al utilizar los recursos y métodos educativos, los padres, madres y profesionales de la educación, pueden ayudar a los jóvenes a desarrollar habilidades digitales positivas. Esta educación es clave para empoderar a los adolescentes y prepararlos para los desafíos del entorno digital actual.

Aquí te presento algunos recursos útiles para la educación digital:

Web de Educación Online



Juegos y App Educativas



Videos y Tutoriales



Charlas y Talleres



Formación



Estas plataformas ofrecen servicios específicos enseñando habilidades sobre seguridad, privacidad y comportamiento responsable en Internet. Visitarlas y explorarlas con nuestros hijos e hijas podría ser una acción muy positiva.

9.3 ¿Cómo nos adaptamos según la edad?

La tecnología está presente y forma parte de nuestra vida diaria desde edades tempranas, os dejamos una guía rápida con una serie de recomendaciones para el uso de la red.



9.4 Ciudadanía e Identidad Digital



En el entorno digital actual, existen una serie de conceptos fundamentales que están estrechamente relacionados y que deben comprenderse de manera conjunta para garantizar una experiencia segura y positiva en Internet.

La expresión "**ciudadanía digital**" se suele utilizar como sinónimo de los términos "**ciberciudadanía**" y "**e-ciudadanía**" para referirse a los derechos y deberes de los ciudadanos en su interacción con la sociedad de la información a través de las tecnologías.

La **Identidad Digital**, por su parte, es el conjunto de informaciones publicadas en Internet sobre mí y que componen la imagen que los demás tienen de mí: datos personales, imágenes, noticias, comentarios, gustos, amistades, etc.

Todos estos datos me describen en Internet ante los demás y determina mi **Reputación Digital**, que es la percepción o imagen que otros tienen de una persona, empresa o entidad en el entorno online, basada en el conjunto de sus interacciones, y contenido compartido en el mundo digital.

**¡¡...Comienza hoy a revisar y mejorar
tu IDENTIDAD DIGITAL...¡¡**



9.5 Construye una Identidad Digital Positiva

Construir una ID positiva es esencial para proyectar una imagen coherente, profesional y respetuosa que favorezca nuestra reputación en plataformas sociales, profesionales y en otros espacios digitales.

A continuación, exploramos una serie de consejos que te ayudarán a construir una buena y positiva Identidad Digital.

- **Creación responsable de perfiles en las RR.SS.** Pensar qué datos se van a publicar en ese perfil y en ocasiones diferenciar entre perfil personal y perfil laboral/académico.
- **Configuración adecuada de la seguridad y privacidad.** Definir de forma correcta las opciones de privacidad del perfil en las RR.SS. Pensar si el contenido a subir es apropiado para difundir en público o sólo en el círculo de amistades.
- **Participación agradable en la Red.** No utilizar un tono maleducado o vejatorio. Mostrar tolerancia y empatía con los demás. No publicar información falsa o advertir del tono de la misma. Pedir permiso a las personas que aparecen en fotos o vídeos antes de subirlas. Ser respetuoso en el empleo de etiquetas en fotos y vídeos.
- **Revisión periódica de la identidad.** Utilizar los buscadores para controlar cada cierto tiempo la información disponible sobre sí mismo en Internet y en especial en las redes sociales.
- **Ayuda.** Acude a tus padres o profesores cuando sospeches que alguien está dañando tu identidad y reputación online.



10

RESPUESTA ANTE UN INCIDENTE

En Internet pueden surgir situaciones inesperadas, responder adecuadamente a un incidente es fundamental para proteger a los jóvenes y minimizar cualquier daño potencial. Aquí hay algunos pasos que tanto los mayores como los más jóvenes usuarios de la red pueden seguir:



Mantén la Calma. respira profundo y evita actuar impulsivamente. La calma te ayudará a seguir estos pasos de manera clara y ordenada.



Bloquea la Actividad Sospechosa: cierra la aplicación o sitio web no respondas ni interactúes con mensajes sospechosos ni con usuarios desconocidos.



Cambia tus Contraseñas: Asegúrate de crear contraseñas seguras que incluyan letras, números y símbolos.



Reporta el Incidente: La mayoría de web, App y RR.SS. tienen opciones para reportar contenido inapropiado, cuentas falsas o actividades sospechosas.



Revisa la Seguridad de tus Cuentas: Activa la autenticación en dos pasos si aún no la tienes configurada.



Comunica el Problema a un Adulto de Confianza: Para menores y jóvenes, informar a un adulto (como un padre, madre, tutor o profesor) es fundamental. Ellos pueden ayudarte a tomar las siguientes decisiones y brindarte apoyo.



Reflexiona y Aprende del Incidente: Habla en familia o con amigos sobre lo ocurrido para que todos aprendan y sepan cómo actuar en el futuro.



Protégete y protege a otros: ante un incidente. ¡ DENÚNCIALO !



10.1 ¿Y si Deseo Presentar una Denuncia?

Si has experimentado o presenciado un ciberdelito es fundamental intervenir rápidamente y de manera efectiva, sobre todo si involucra a menores de edad, siguiendo ciertos pasos podrás garantizar que se tomen las acciones necesarias para protegerlos y abordar el problema.

ACTÚA...

1. Mantén la calma y evalúa la situación.

Actúa de manera reflexiva y cuidadosa, cada detalle es importante.

2. Recopila evidencias y datos.

Guarda capturas de pantalla, Mensajes, URL, incluyendo fechas.

3. Contacta con las FFCCS.: Guardia Civil / CNP.

Utiliza canales oficiales: Presencial en Cuarteles / WEB Online.

4. Describe el incidente con claridad.

Explica los hechos de forma clara y ordenada, aporta toda la información que puedas (Web, Perfil, Datos de contacto).

5. Solicita asistencia CIBER-especializada.

Si tienes dudas sobre el proceso, consulta online o pide apoyo a través de las Líneas de Ayuda en ciberseguridad.

6. Si en el incidente está involucrado algún menor.

No compartas detalles de la denuncia, mantén la privacidad, y si es necesario busca apoyo emocional de un experto o profesional.

RECUERDA....

**Actuar rápido y seguro puede ayudar a resolver el incidente
y prevenir futuros problemas.**



10.2 ¿Dónde y de qué forma Denunciar?

› ¿Qué es una denuncia?

Es la información que facilita una persona a los agentes de la autoridad o funcionarios, que actúan como receptores de la misma, para poner en conocimiento de la autoridad competente un hecho o una omisión que él considera que es contraria a la Ley.

› ¿Cómo se denuncia?

- **Por escrito:** Mediante la presentación de un escrito, el cual deberá estar firmado por la persona que lo realiza y previa identificación.
- **Verbalmente:** Ante los agentes de la autoridad o funcionario que recoge la manifestación de los hechos denunciados por escrito.
- **Vía Telemática:** A través de la aplicación E-DENUNCIA, presentación de una denuncia de forma electrónica.

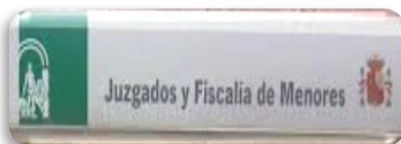
› ¿Ante quién se puede denunciar?

Ante las autoridades, funcionarios y agentes competentes que están encargados de investigar y sancionar el hecho u omisión presuntamente ilegal.



INFORMACIÓN

Existe un **protocolo** de actuación a adoptar por los Centros Educativos en situaciones de **ciberacoso**.
(Inst. 11/01/17)
Junta de Andalucía
Consejería de Educación





10.3 Líneas de Ayuda

En esta sección se detallan las principales Líneas de Ayuda relacionadas con la ciberseguridad, ofreciendo orientación y apoyo en tiempo real, así como información preventiva y asesoramiento para fomentar un uso seguro y responsable de Internet.



CONCLUSIONES



El avance de la tecnología y el acceso a Internet han transformado la forma en que los menores interactúan, aprenden y se entretienen. Por ello, es fundamental comprender que la ciberseguridad es una responsabilidad compartida y que trabajar juntos en su implementación puede marcar una gran diferencia en la protección y el bienestar digital de los niños y niñas.

Educación y Conciencia: Es crucial educar a los menores sobre los riesgos en línea y cómo actuar ante situaciones potencialmente peligrosas. Del mismo modo, padres, madres y educadores deben actualizarse continuamente sobre tendencias digitales para poder guiar y proteger de manera efectiva.

Comunicación Abierta: Fomentar un ambiente donde los menores se sientan cómodos hablando de sus experiencias en línea es esencial.

Herramientas de Protección: Aprovechar las herramientas de control parental, configuraciones de privacidad y software de seguridad es un paso básico pero crucial.

Respeto y Empatía Digital: Enseñar a los menores a respetar a los demás en el entorno digital contribuye a un espacio más seguro para todos. Combatir el ciberacoso y promover un comportamiento ético online debe ser una prioridad.

En conclusión, Los adultos deben ser modelos de comportamiento digital responsable. Proteger a los menores en el ámbito digital no es solo una tarea técnica, sino también educativa y emocional. Este manual busca ser un recurso para empoderar a todas las partes involucradas, brindándoles las herramientas necesarias para navegar en el mundo digital de manera segura, responsable y consciente. Al trabajar juntos, podemos construir un entorno online más seguro y enriquecedor para todos.



“Cuidar de los menores en el mundo digital es proteger su presente y construir su futuro.”

¡Gracias!

La seguridad en el entorno digital comienza con pequeños pasos, y este manual es uno de ellos. Al trabajar juntos, padres, madres, educadores y menores podemos construir una experiencia que sea no solo segura, sino también enriquecedora y llena de oportunidades.

Para más información:

- Referencia: **Comandancia Guardia Civil de Córdoba – Equipo @**
- Línea de ayuda: **957 414111 Ext. 0440296**
- Contacto directo: **cordoba-equipo@guardiacivil.org**

Escanea este código para acceder al manual en formato digital



Comandancia de la Guardia Civil de Córdoba
Equipo @
Avda. Medina Azahara, 2
14005, Córdoba