



IES MIGUEL ESPINOSA



PLAN DIGITAL

DESARROLLO DE LA CONCIENCIA DIGITAL.
PRÁCTICAS SALUDABLES

DESARROLLO DE LA CONCIENCIA DIGITAL. PRÁCTICAS SALUDABLES

La conciencia digital representa el conocimiento de los riesgos y oportunidades que presenta la tecnología para su uso eficaz y responsable. Temas como el bienestar digital, la ciberseguridad, la información fiable y la protección de datos forman parte de este concepto tan importante en la sociedad actual.

Bienestar digital

El bienestar digital es la búsqueda de una relación intencional y sana con la tecnología en el lugar de trabajo y en la vida personal. La necesidad de bienestar digital corresponde a las muchas facetas en que el uso poco consciente de las tecnologías digitales puede afectar a nuestra salud:

Fatiga visual

Un tiempo excesivo ante la pantalla puede forzar los músculos implicados en el foco ocular y provocar tensión ocular. Además, al mirar pantallas digitales, el ojo no parpadea tan a menudo y esto provoca sequedad en los ojos e irritaciones oculares menores. Hay que descansar los ojos cada cierto tiempo o, incluso, hacer determinados ejercicios.

Insomnio

Fenómeno que afecta especialmente a las personas más jóvenes; hay estudios que concluyen que el 77% del colectivo adolescente sufre problemas de sueño. Sesiones largas de juegos o notificaciones frecuentes recibidas en el teléfono durante la noche pueden alterar nuestros patrones de sueño.

Disminución de la atención

Tener dispositivos digitales alrededor, sobre todo si las notificaciones están activadas, afecta nuestra capacidad de mantener la concentración. Además, algunas aplicaciones que requieren atención, tales como aplicaciones de redes sociales, intentan crear un hábito al usuario o usuaria para que éste compruebe la aplicación constantemente.

Disminución de la creatividad

La estimulación constante que proporciona el mundo digital se puede utilizar como fuente de inspiración, pero también puede reducir la creatividad si el usuario consume pasivamente el contenido y reduce el tiempo de soledad, contemplación y reflexión.

Ciberbullying

Estudios recientes indican que los adolescentes que pasan más horas al día conectados tienen más probabilidades de sufrir ciberacoso o ciberbullying ya que el abuso se recibe a través de dispositivos que acompañan a las víctimas en todo momento.

Las mejores prácticas para abordar estos problemas relacionados con la salud en relación con el uso de las tecnologías tienen como objetivo mantener un equilibrio razonable entre salud y conectividad. Reducir el tiempo de pantalla, bloquear notificaciones no esenciales o configurar los teléfonos móviles en modo avión durante las horas de productividad y el tiempo de reposo son ejemplos de buenas prácticas hacia el bienestar digital.

Ciberseguridad

La ciberseguridad, también denominada seguridad de la información, es la práctica para garantizar la integridad, confidencialidad y disponibilidad de la información. Implica un conjunto de herramientas, formación y buenas prácticas diseñadas para proteger las redes, los dispositivos, los programas y los datos contra ataques o accesos no autorizados.

Las principales amenazas a la ciberseguridad aparecen en forma de software malicioso, como virus informáticos, programas espía (spyware), Troyanos y registro de claves (keylogger). Estos programas suelen tener como objetivo permitir el control remoto de los dispositivos atacados, dañarlos y / o extraer información.

La conciencia digital relacionada con la ciberseguridad implica un conjunto de buenas prácticas, tales como:

Contraseñas fuertes

El uso de contraseñas seguras que combinan letras, números y caracteres especiales es clave para evitar el acceso no deseado a nuestras cuentas e información personal. La longitud de la contraseña también es importante. Se recomienda utilizar una contraseña diferente a cada cuenta para reducir los daños cuando una contraseña se ve comprometida. También es importante prestar atención a cualquier pista que pueda ser indicativo de un acceso externo no deseado en nuestra cuenta, y cambiar las contraseñas periódicamente.

Evitar las redes Wi-Fi abiertas

Las conexiones Wi-Fi en lugares públicos son propensas a ataques, por lo que es recomendable no utilizarlas, especialmente aquellas que no implementan funciones de seguridad. Si se utiliza este tipo de redes Wi-Fi abiertas, es necesario tener precaución al acceder a cualquier página web y asegurarse de que al menos la navegación segura (direcciones web empezando por HTTPS y con un certificado

válido) está habilitada. En todos los casos, hay que evitar acceder a información sensible (por ejemplo, cuentas bancarias) en una Wi-Fi pública, así como desactivar la interfaz Wi-Fi cuando no se utilice.

No compartir información personal

Tener precaución a la hora de compartir cualquier tipo de información personal en línea es una buena práctica, poniendo especial atención en las redes sociales, las empresas y las personas que se ponen en contacto con nosotros.

Comprobar la identidad

Es importante comprobar la oficialidad de las cuentas corporativas y la veracidad de los perfiles individuales con los que contactamos en línea para evitar ataques de suplantación y de ingeniería social.

Información fiable

La información fiable es la información extraída de fuentes oficiales y contrastadas, frente a fenómenos en línea como las noticias falsas y la desinformación. La capacidad de comprobar la veracidad de la información obtenida en línea es necesaria para contrarrestar la creciente difusión viral de la información falsa que cultivan las redes sociales.

Es importante conocer las herramientas para la búsqueda de información fiable, ya que la difusión de noticias falsas puede, incluso, amenazar la seguridad individual de las personas.

Buenas prácticas para la búsqueda de información fiable

- Lee el artículo completo. Ve más allá del titular y intenta entender toda la historia.
- Comprueba las fuentes. Busca si las fuentes son fiables y si coinciden con el artículo.
- Comprueba la fecha. Comprueba si la información está actualizada o si la información está aún vigente.
- Considera si el contenido del artículo transmite información real o es una broma.
- Sé neutral. Procura no ser sesgado cuando busques información. Busca los hechos verdaderos, independientemente de si coinciden o no con tus creencias anteriores.
- Consulta expertos. Comprueba lo que lees con expertos sobre el tema.

Protección de Datos

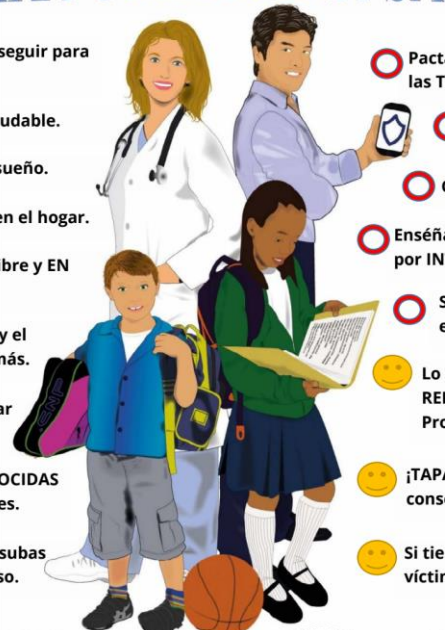
La protección de datos, también conocida como privacidad de la información, está relacionada con el tratamiento adecuado de datos personales y confidenciales que las entidades en línea deben seguir para proteger estos datos, de modo que no se compartan o se filtren de manera indebida .

Es necesario entender los derechos de protección de datos y leer atentamente los términos y condiciones del acuerdo de cada servicio en línea, ya que el hecho de compartir nuestros datos personales con terceros puede afectar nuestra privacidad y huella digital en línea, o incluso, puede utilizarse para manipularnos o engañarnos en el futuro.

La información personal se utilizará de forma que garantice la seguridad adecuada, incluida la protección contra procesos, accesos, pérdidas, destrucciones o daños efectuados de forma ilegal o no autorizada.

Ínfografía del Ministerio del Interior del Gobierno de España que resume las principales actuaciones que deben seguirse para una buena salud digital

CONSEJOS PARA UNA BUENA SALUD DIGITAL



- +** Recuerda que eres el **EJEMPLO** a seguir para tus hijos.
- +** Fomenta hábitos de vida saludable.
- +** Respeta las horas de sueño.
- +** La igualdad de género empieza en el hogar.
- +** Fomenta actividades al aire libre y **EN FAMILIA**.
- +** Fomenta la empatía, la igualdad y el respeto a los derechos de los demás.
- 😊** La **SEGURIDAD** empieza por usar **CONTRASEÑAS** complejas.
- 😊** **NO** aceptes a **PERSONAS DESCONOCIDAS** en tus redes sociales y aplicaciones.
- 😊** **RESPETA** a los demás y no subas imágenes tuyas sin permiso.
- ⦿** Pacta normas con tus hij@s sobre el uso de las TIC.
- ⦿** **SUPERVISA** lo que **HACE** tu hij@ cada vez que se conecta a la RED.
- ⦿** Comparte sus **GUSTOS** y **AFICIONES**.
- ⦿** Enséñale a navegar de forma **RESPONSABLE** por **INTERNET**.
- ⦿** Sitúa los **DISPOSITIVOS ELECTRÓNICOS** en un lugar de uso común.
- 😊** Lo que **SUBES** a la RED, se **QUEDA EN LA RED**. No facilites información personal. Protege **TU PRIVACIDAD**.
- 😊** ¡**TAPA TU WEBCAM!** Podrían acceder a ella y conseguir imágenes tuyas.
- 😊** Si tienes problemas pide ayuda y si eres víctima de un delito ¡**DENUNCIA!**

200 POLICIA NACIONAL
www.policia.es

Familia y Salud
www.familiaysalud.es

SEPS
Servicio Español de Pediatría Social
www.pediatriasocial.es

AEP
Asociación Española de Pediatría
www.aeped.es

AEPap
Asociación Española de Pediatría de Atención Primaria
www.aepap.es

U23
GOBIERNO DE ESPAÑA
MINISTERIO DEL INTERIOR
DIRECCIÓN GENERAL DE LA POLICIA
<https://cpag.mpr.gob.es/>

NPPO (copyleft) ISBN-25-0863-8 DEPOSITO LEGAL: M-22342-2023 NPPO (cod. en línea) ISBN-25-0863-8