1.5.3. Ciberseguridad. Bienestar digital. Riesgos de la red.

Ciberseguridad

> ¿A qué nos referimos cuando hablamos de **ciberseguridad?** Nos referimos a las **medidas** y prácticas utilizadas para **proteger** los **sistemas informáticos, redes** y **datos** de posibles amenazas o ataques cibernéticos. Incluye la **protección de la información confidencial**, la **prevención de accesos no autorizados**, la **detección de actividades maliciosas** y la **respuesta ante incidentes de seguridad**. La ciberseguridad abarca tanto a nivel personal, en la protección de nuestros dispositivos y datos personales, como a nivel empresarial, donde se busca salvaguardar la información de la organización y proteger su infraestructura tecnológica.

En la página del **INCIBE (Instituto Nacional de Ciberseguridad)** podemos encontrar mucha **ayuda** con respecto a estas cuestiones. Resulta prácticamente imposible decantarse por una u otra guía, pues todas son muy interesantes y necesarias. Puedes elegir aquella que consideres más necesaria o de mayor interés para ti en este momento o ir leyendo todas poco a poco. También encontrarás muchos recursos para trabajar con tu alumnado (fichas, talleres, recursos descargables, actividades interactivas, test de autoevaluación).

	En esta guía del INCIBE encontramos las claves para respaldar fácilmente la información almacenada en dispositivos Windows, Mac, Android e iOS.

En estas fichas del INCIBE encontramos información sobre las características de los navegadores más utilizados, especialmente las relacionadas con aspectos de privacidad y seguridad.

Esta guía de ciberseguridad del INCIBE está pensada para los más mayores, pero es muy completa e interesante, así que, si encuentras tiempo y tienes interés en ampliar y afianzar tus conocimientos al respecto: te recomendamos su lectura.

Esta guía del INCIBE está formada por 18 fichas que recogen los principales riesgos a los que nos exponemos al hacer uso de Internet así como las medidas de protección que debemos aplicar para evitarlos.

En este recurso se nos muestran tres situaciones típicas con las que cualquier usuario de una red social se ha encontrado una vez. Se trata de seguir el árbol de decisiones para tomar siempre el camino correcto y navegar seguro por las redes sociales.

Es una aplicación gratuita que ayuda a proteger el dispositivo móvil Android. Permite conocer el estado de seguridad del dispositivo, mostrando soluciones a posibles riesgos a los que esté expuesto y proporcionando algunos consejos que ayudarán a mejorar su seguridad.

Bienestar digital

> ¿A qué nos referimos cuando hablamos de **bienestar digital**? El bienestar digital se refiere al **estado de equilibrio y bienestar** de las personas **en relación con su uso de la tecnología digital**.

El bienestar digital implica adoptar **hábitos y prácticas saludables** en relación con la **tecnología,** como establecer **límites** en el tiempo de uso, **desconectarse** regularmente, tener **períodos de descanso** adecuados, **evitar la adicción** a los dispositivos y **promover** un **uso responsable** de la tecnología.

Además, el bienestar digital también se refiere a la **capacidad** de utilizar la tecnología de manera **productiva** y **positiva,** como utilizarla para el **aprendizaje,** el **crecimiento personal,** la **comunicación** y el **desarrollo de habilidades.** También implica la búsqueda de un **equilibrio** entre el uso de la tecnología y otras actividades importantes en la vida cotidiana, como el trabajo, el tiempo en familia, el ejercicio físico y el tiempo al aire libre. En definitiva, **se trata de utilizar la tecnología de manera consciente y equilibrada, para que beneficie a nuestra salud y calidad de vida, en lugar de perjudicarla.**

Cómo mejorar el bienestar digital

> Prestar atención a los siguientes aspectos puede ayudarnos a **mejorar nuestro bienestar digital:**

- **Límites de tiempo de exposición a las pantallas**: Es importante establecer límites y horarios para el uso de dispositivos digitales. Esto evitará la sobreexposición y nos permitirá dedicar tiempo a otras actividades importantes.

https://www.youtube.com/embed/f0_2XBod8Hg

- **Gestión del tiempo**: Organizar y administrar nuestro tiempo en línea de manera eficiente es fundamental. Establecer una agenda y priorizar las tareas ayudará a evitar la sensación de estar siempre conectados.
- **Privacidad y seguridad en línea**: Mantener nuestros datos personales seguros y protegidos es esencial. Utilizar contraseñas fuertes, evitar compartir información sensible y revisar regularmente las configuraciones de privacidad en las redes sociales son algunas medidas que podemos tomar.

https://www.youtube.com/embed/4YSGMBv56Ec

- **Desconexión:** Es importante permitirnos momentos de desconexión digital. Esto puede incluir períodos de tiempo sin dispositivos electrónicos, como apagar el teléfono durante la noche o los fines de semana.

https://www.youtube.com/embed/3jEosMJEyK4

- **Socialización equilibrada**: Las relaciones sociales digitales son importantes, pero también debemos fomentar los encuentros en persona y la comunicación cara a cara. Encontrar equilibrio entre nuestras interacciones en línea y fuera de línea es esencial para nuestro bienestar.

https://www.youtube.com/embed/eo14JAmkvs4

- **Control de la información consumida**: Es crucial ser selectivos con la información que consumimos en línea. Elegir fuentes confiables, evitar la sobreexposición a noticias negativas y mantener una actitud crítica hacia la información que encontramos ayudará a mantener una perspectiva saludable.
- **Cuidado de nuestra salud física**: El uso prolongado de dispositivos digitales puede tener un impacto en nuestra salud física. Es importante cuidar nuestra postura, hacer pausas regulares para levantarnos y estirarnos, y mantener una rutina de ejercicio físico.

https://www.youtube.com/embed/wJHbD6CGQDs

- **Autoevaluación:** Regularmente debemos evaluar cómo nos sentimos en relación con nuestro uso de dispositivos digitales. Si sentimos que estamos haciendo un uso excesivo o que nuestra relación con la tecnología es negativa, es importante buscar apoyo y ayuda profesional si es necesario.

Riesgos de la red

¿Aquénosreferimoscuandohablamosde" **riesgosdela red**"? Nos referimos a los **peligros** o **amenazas** que pueden surgir al **utilizar Internet** y las **tecnologías digitales** en el ámbito educativo.

Estos riesgos pueden afectar tanto a **docentes** como a **estudiantes** y pueden incluir:

- **Contenido inapropiado**: Acceder a información, imágenes o videos que sean inapropiados para la edad y el nivel de madurez de los estudiantes.

https://www.youtube.com/embed/5HWBDPW3xbQ

- **Ciberacoso:** Ser víctima de intimidación, humillación o acoso a través de las redes sociales, mensajes de texto u otras plataformas en línea.

https://www.youtube.com/embed/G8iciqvXnmk

- **Robo de identidad**: Que alguien pueda utilizar de manera fraudulenta los datos personales o contraseñas de los estudiantes o docentes.
- **Engaños y estafas**: Ser víctima de fraudes en línea, donde se solicitan datos personales, o se realizan compras falsas, entre otros.
- **Adicción a internet y las redes sociales**: Desarrollar una dependencia excesiva o compulsiva hacia las tecnologías y las redes sociales, lo que puede afectar el rendimiento académico y la salud mental de los estudiantes.

https://www.youtube.com/embed/lyOoHtyyI0U

https://www.youtube.com/embed/Gh2LJGQc9t8

- **Falta de privacidad**: Compartir demasiada información personal en línea, sin tener en cuenta los riesgos de que sea utilizada de manera indebida.

https://www.youtube.com/embed/SiqpwmTpb68

- **Violencia en línea**: Exponerse a contenidos violentos, como imágenes de agresiones físicas, incitación al terrorismo o juegos que promueven la violencia.
- **Falsificación de identidad**: Suplantar la identidad de otra persona, haciéndose pasar por ella en internet.

https://www.youtube.com/embed/i_92-NovRT0

> Es importante que estudiantes y docentes estén conscientes de estos riesgos y tomen medidas para protegerse a sí mismos y a los demás mientras usan internet y las TIC en el contexto educativo.

Podríamos agrupar estos **riesgos** en torno a:

1. Acceso a **contenido no apropiado** para menores.
2. **Ciberacoso.**
3. **Adicción** a las redes sociales.
4. **Riesgos de seguridad informática**: las redes y los dispositivos móviles son vulnerables a los ataques cibernéticos como la suplantación de identidad, la interceptación de comunicaciones, las amenazas de malware y la exposición de información personal.
5. **Falta de control parental**.

> Es importante que se implementen medidas preventivas y de seguridad en el ámbito educativo para hacer frente a estos riesgos y garantizar un entorno de aprendizaje seguro y saludable para los estudiantes.

Ciberseguridad en el puesto de trabajo

Compartimos este documento sobre **ciberseguridad en el puesto de trabajo** elaborado por **Eloy Villa,** experto en ciberseguridad, como resumen del asesoramiento realizado a docentes en el marco de una actividad para la formación del profesorado en este ámbito.

GUÍA - RESUMEN
CIBERSEGURIDAD EN EL PUESTO DE TRABAJO

Material de la sesión formativa asociada a la actividad nº 9506 (DOCEO) realizada con el personal del Equipo de Orientación Educativa de Atención Temprana

CONTRASEÑAS

- ☐ Usar una contraseña fuerte (8-10 caracteres, con MAYUSCULAS, minúsculas, números y símbolos especiales, como . , - $ % & ( ) @#)
- ☐ No usar la misma contraseña para todo
- ☐ Se puede pensar en usar un patrón, como por ejemplo, una palabra, con las vocales en minúsculas, las consonantes en mayúsculas, un año partido en 2 partes y un símbolo especial, añadiendo una 't' para Twitter, una 'f' para Facebook, una 'g' para Gmail, …
- ☐ Por ejemplo: 20eJea23#.t para Twitter, 20eJea23#.f para Facebook, etc.
- ☐ No dejar las contraseñas a la vista (post-its, apuntes, fichero con contraseñas en el escritorio, …

CORREO ELECTRÓNICO

- ☐ Prestar atención al dominio de donde viene un correo (Ej. En juan@gmail.com el dominio es Gmail.com, que es conocido y fiable). Si no se ve, desplegar la cabecera para ver más detalles
- ☐ Especial atención a los enlaces que vienen dentro del correo. Si se pone el ratón sobre ellos sin hacer click, aparece un rectángulo gris con la información real del enlace a donde nos lleva.
- ☐ Cuidado con los ficheros adjuntos. Revisar si son docx (documentos Word), pdf (se abren con el Adobe Reader), xls (ficheros Excel), jpg (imágenes), … aunque hay muchos más. Revisar qué es antes de abrirlos.
- ☐ Si nos solicitan datos bancarios, privados o sensibles, podemos hacer la comprobación por teléfono antes de mandarlos, llamando a la persona que nos lo solicita por teléfono y confirmar que realmente es esa persona la interesada.
- ☐ Las tildes mal escritas pueden ayudar a identificar correos maliciosos.
- ☐ Si algo se sale de lo normal, sospechar siempre.
- ☐ Se puede ampliar más información en la web oficial de Microsoft, visionando unos vídeos muy cortitos en esta dirección:

https://support.microsoft.com/es-es/windows/prot%C3%A9jase-del-phishing-0c7ea947-ba98-3bd9-7184-430e1f860a44

COPIAS DE SEGURIDAD

- ☐ Regla del 3-2-1: mantener 3 copias "vivas". Al hacer la 4ª se puede eliminar la más antigua. En 2 dispositivos distintos (2 pendrives diferentes y en diferentes lugares). 1 vez por semana (recomendable)
- ☐ Las políticas de la copia de seguridad pueden variar dependiendo de la carga de trabajo (si se hace mucha documentación un día puede ser interesante hacer una copia ese día sin esperar al día programado.

CLOUD / NUBE

- ☐ Se puede hacer uso de la nube para mantener copias de seguridad en One Drive o Google Drive
- ☐ Los programas agentes sincronizadores pueden ser útiles, pero personalmente, prefiero subir manualmente los documentos a la nube.
- ☐ Tener en cuenta que lo que se sube a la nube si está compartido, se hace público. Compartir sólo lo que sea necesario, y si se comparte una carpeta completa, asegurarse de que en dicha carpeta no se sube material personal o sensible.

TELÉFONOS MÓVILES

- ☐ Eliminar todas las wifis que no se necesiten tener almacenadas
- ☐ Instalar un programa antivirus como ESET o CONAN MOBILE
- ☐ Revisar los permisos que otorgamos a las aplicaciones al instalarlas. CONAN MOBILE puede ayudarnos con esto.
- ☐ Mantenerlo actualizado, tanto el propio sistema Android como las aplicaciones

- ☐ Decidir si es necesario o no tener activos los asistentes de voz, como Siri, Alexa, Cortana, Ok Google, …

CIFRADO

- ☐ Cifrar con la utilidad en Android la memoria del teléfono (en ajustes -> almacenamiento -> cifrado de memoria) (la ruta puede variar según dispositivos)
- ☐ Si en Windows no aparece en cifrado de BitLocker, puede que sea que no está disponible para la versión Home de Windows. Podemos activarlo siguiendo estos pasos de la web de Microsoft:

https://support.microsoft.com/es-es/windows/activar-el-cifrado-de-dispositivo-0c453637-bc88-5f74-5105-741561aae838#ID0EBD=Windows_10

o en la versión de Windows 11:

https://support.microsoft.com/es-es/windows/activar-el-cifrado-de-dispositivo-0c453637-bc88-5f74-5105-741561aae838#ID0EBD=Windows_11

- ☐ Sería importante cifrar los pendrives que vayan a salir de la oficina, por si se pierden, que quien los encuentre no pueda acceder a la información del mismo.

PUESTO DE TRABAJO

- ☐ Mantener el puesto de trabajo con la mínima información sensible expuesta (informes, documentos, post-its, …) para evitar que posibles visitas o trabajadores ajenos al departamento accedan a dicha información.
- ☐ Si tenemos que irnos de nuestro puesto de trabajo, podemos bloquear la sesión pulsando las teclas

(Recordad el ataque David Hasselhoff con los Perritos)

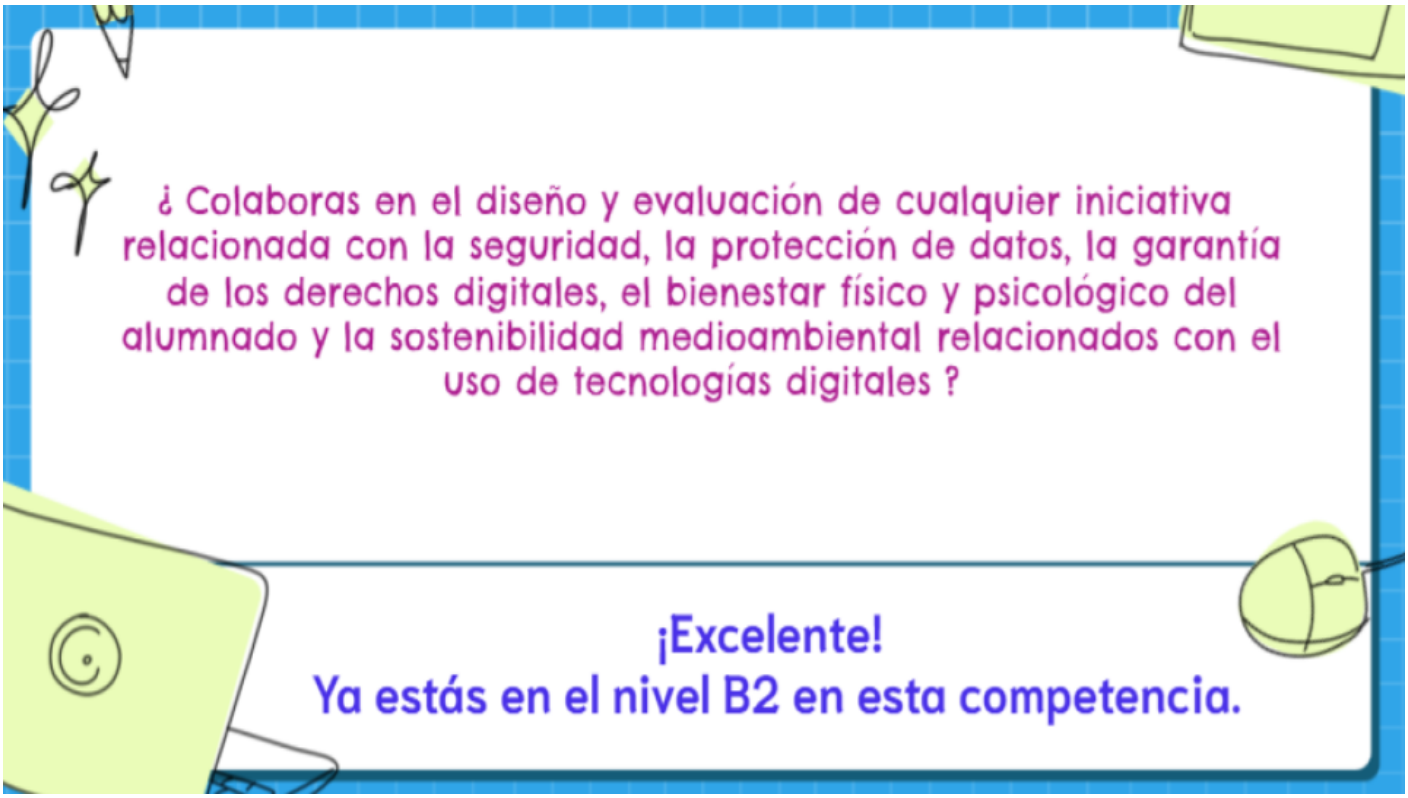
NAVEGADOR DE INTERNET

- ☐ Revisar la ruta de las webs que estemos visitando.
- ☐ Recordar que el candadito verde no quiere decir que la web sea buena, si no que la comunicación es cifrada, sólo eso
- ☐ Si la web que estamos visitando no tiene el certificado correcto (es http en vez de https o tiene el certificado caducado), es un riesgo seguir navegando en dicha web.
- ☐ Podemos trabajar en “modo incógnito”, abriendo Google Chrome y pulsando las teclas

El modo incógnito no nos protege de nada, sólo nos hace no cargar cookies, ni historial de navegación, ni historial de búsquedas. Puede no ser útil si tenemos que volver a trabajar en ese equipo, pero tenemos la privacidad de que si la siguiente persona que use el equipo no es de confianza no tendrá esa información privada nuestra.

- ☐ Recordad cerrar sesión siempre que ya no necesitéis tener acceso a la web que sea, más aún si no es en nuestro equipo donde la hemos abierto.

Imagen: Eloy Villa, experto en ciberseguridad (informaticaeloy.com). CC-BY-NC-SA.



Revision #15
Created 2023-04-07 00:59:13 CEST by María Esther Arilla Luna
Updated 2023-11-03 12:16:34 CET by María Esther Arilla Luna