Protección de Datos Personales, Privacidad, Seguridad y Bienestar Digital

Introducción

Esta es la úlltima competencia del *Área 1. Compromiso profesional* del Marco Digital Docente. Aquí abrazamos todo lo realizado anteriormente bajo el paraguas de la seguridad y el bienestar. Como docentes tenemos una gran responsabilidad con la cantidad de información a la que tenemos acceso, y es por eso que esta competencia es de vital importancia para entender la importancia de salvaguardar la información de propios y terceros (alumnado, familias..).

> Proteger los datos personales, las comunicaciones y el acceso a los dispositivos, dentro del ámbito educativo, para evitar los riesgos y amenazas que afecten a los derechos y garantías digitales de todos los miembros de la comunidad educativa contemplados en la normativa vigente. Utilizar de manera responsable, segura y saludable las tecnologías digitales para evitar riesgos laborales, personales y en el entorno y para garantizar el bienestar físico, psicológico y social del alumnado al utilizar las tecnologías digitales.

Esta competencia se concreta en la aplicación de las medidas y protocolos de seguridad en el centro, que deben desarrollar los establecidos por la legislación vigente. Aquí el plan digital del centros se presenta como un documento de centro donde alojar todos estos protocolos, ya que en él se deberá recoger el conjunto de medidas que garanticen el bienestar de la comunidad educativa.

Seguridad y privacidad en internet

Pese a ser dos conceptos distintos, Seguridad y Privacidad van íntimamente relacionados. Conocer y aplicar normas de seguridad en internet, nos permitirá mantener a salvo nuestra privacidad y la de nuestra información.

A continuación, vamos a ver una serie de consejos para mantener a salvo nuestra privacidad:

Contraseñas seguras y robustas:

> Una de las primeras barreras más importantes para evitar el uso fraudulento de nuestra identidad es tener una contraseña robusta y difícil de descifrar. Aquí te ponemos algunas características que una contraseña debería tener para responder a los criterios mínimos de seguridad.

1. CUALIDADES QUE DEBERÍA CUMPLIR UNA CONTRASEÑA:

- **Debemos asegurarnos que la contraseña tenga** una:
  - longitud mínima de doce caracteres,
  - que combine mayúsculas,
  - minúsculas,
  - números y
  - símbolos.
- **No debemos utilizar como claves:**
  - palabras sencillas en cualquier idioma,
  - nombres propios,
  - lugares,
  - combinaciones excesivamente cortas,
  - fechas de nacimiento,
  - etc.
- **Tampoco debemos usar claves formadas únicamente a partir de la concatenación de varios elementos**. Por ejemplo: “Juan1985” (nombre + fecha de nacimiento).

2. CUALIDADES QUE UNA CONTRASEÑA NO DEBERÍA TENER

Ejemplo de cómo deben ser las contraseñas

Oficina de seguridad del internauta. Imagen monográfico que deberías saber contraseñas ejemplos. https://www.osi.es/sites/default/files/quedeberiassaber/imagen-monografico-que-deberias-saber-contrasenas-ejemplos.png

> Dentro de este artículo *https://www.osi.es/es/contrasenas* hacen el siguiente análisis de **cuanto tardaría un software** de combinación de caracteres en adivinar una contraseña **dependiendo de la combinación** que realizamos con los caracteres. Por un lado sería mezclando mayúsculas y minúsculas (todos los caracteres) y por otro solo minúsculas:

Longitud	Todos los caracteres	Sólo minúsculas
3 caracteres	0,86 segundos	0,02 segundos
4 caracteres	1,36 minutos	0,46 segundos
5 caracteres	2,15 horas	11,9 segundos
6 caracteres	8,51 días	5,15 minutos
7 caracteres	2,21 años	2,23 horas
8 caracteres	2,10 siglos	2,42 días
9 caracteres	20 milenios	2,07 meses
10 caracteres	1.899 milenios	4,48 años
11 caracteres	180.365 milenios	1,16 siglos
12 caracteres	17.184.705 milenios	3,03 milenios
13 caracteres	1.627.797.068 milenios	78,7 milenios
14 caracteres	154.640.721.434 milenios	2.046 milenios

https://www.osi.es/es/contrasenas

Estrategias para generar contraseñas

Una vez visto que cualidades debe cumplir una contraseña para ser segura, vamos a ver diferentes estrategias para que además de ser segura también sea fácil de recordar y útil para nosotros. Es importante que cualquier **contraseña siga un proceso cognitivo lógico** para que si no recordamos exactamente los elementos de la contraseña, mediante el razonamiento lógico seamos capaces de deducirla.

> a Consejo: Utilizar **contraseñas diferentes para diferentes plataformas** que utilicemos, ya que si se produce un grieta de seguridad en alguna de nuestras cuentas yquedamos descubiertos, estas credenciales servirían para poder entrar en el resto de cuentas.

En ocasiones, recordar todas las contraseñas que utilizamos (correo electrónico, redes sociales, mensajería instantánea, foros, etc.) puede resultar complicado. Para facilitar la tarea, podemos utilizar algunas sencillas reglas:

- **Cambiar las vocales por números**. Por ejemplo:
  - Mi familia es genial → M3 f1m3l31 2s g2n31l
- **Utilizar reglas mnemotécnicas**. Por ejemplo, elegir la primera letra de cada una de las palabras de una frase que sea fácil de recordar para nosotros:
  - Con 10 cañones por banda… → C10cpb…
- **Para hacer más sencillo el trabajo, podemos utilizar claves basadas en un mismo patrón, introduciendo ligeras variaciones para cada servicio**. Por ejemplo, tomando como base la contraseña anterior, añadir al final la última letra del servicio utilizado en mayúscula:
  - Facebook → C10cpb…K
  - Twitter → C10cpb…R
  - Gmail → C10cpb…L
- **Dependiendo del servicio y de su importancia podemos utilizar claves más robustas o menos, para facilitar su memorización.** Para los servicios más sensibles, siempre podemos utilizar un generador aleatorio de contraseñas. La mayoría de los gestores de contraseñas ofrecen esta funcionalidad.

> Otra razón para no utilizar la misma clave en diferentes servicios es el hecho de que **algunos** de ellos **no almacenan nuestra contraseña cifrada en sus servidores.** En este caso, involuntariamente la estamos compartiendo con estos servicios, por lo que debemos poner una contraseña que no se parezca a ninguna de las otras que utilizamos. Una pista **para poder identificar estos servicios es comprobar si al darnos de alta o recuperar la contraseña nos indican cual era nuestra clave**, en lugar de proporcionarnos un enlace para cambiarla.

Ayúdate de un gestor de contraseñas:

En la actualidad, manejamos distintas contraseñas para cada una de las actividades que realizamos: compras online, plataformas de streaming, correos electrónicos, gestiones bancarias.... todas y cada una han de ser distintas y cumplir unas condiciones muy particulares (mayúsculas, número de caracteres, con/sin símbolos...).

Por ello, los gestores de contraseñas se vuelven poderosos aliados ayudándonos a generar contraseñas tan seguras como aleatorias, y a tenerlas almacenadas para cuando nos son

requeridas.

> Utiliza sólo gestores de contraseña en tus dispositivos personales y no en aquellos de uso público.

A continuación, encontrarás cinco gestores de contraseñas gratuitos y de código abierto:

- Keepass
- Bitwarden
- Passbolt
- Psono
- Teampass

Antivirus

Un antivirus es un software que protege nuestro dispositivo de programas malignos como **virus, spyware, gusanos, troyanos, rootkits**, etc. Además de **buscar y detectar** amenazas cuando se lo solicitamos, nos ofrecen **protección en tiempo real**.

Es imprescindible que estén siempre actualizados, por lo que se recomienda tener activada la **actualización automática** de modo que, cada vez que se inicie el ordenador, busque si hay actualizaciones pendientes y las instale.

Recuerda que el software malicioso no afecta sólo a los ordenadores, por lo que debes tenerlo instalado también en el resto de dispositivos que utilices (ej: smartphone)

Corta fuegos

La función del cortafuegos (o firewall, en inglés) es permitir, limitar, cifrar y descifrar el tráfico entrante en un sistema de información, bloqueando el acceso de personas o software externo no autorizado a nuestro ordenador y controlando también la información que diversos tipos de software puedan enviar desde nuestro ordenador, en sentido contrario.

Cuando un software es de confianza y requiere enviar y recibir información, debemos agregarlo a la lista de excepciones de nuestro cortafuegos.

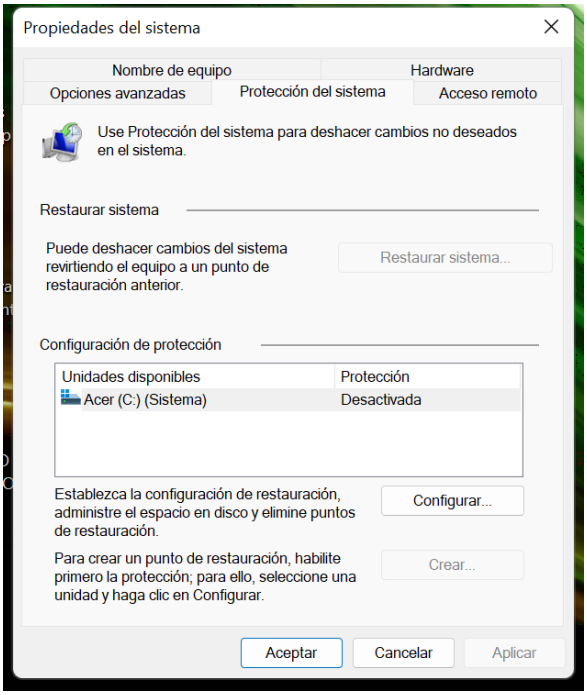
La protección del cortafuegos se limita únicamente a la información que viene a través de internet, no surtiendo efecto ante posibles infecciones por instalación local de software malicioso que pueda provenir, por ejemplo de un pendrive (en ese caso, el encargado de actuar es el antivirus).

Copias de seguridad

Ir haciendo copias de seguridad del material más importante es una buena manera de prevenir la pérdida de esta información si se diera una infección. Podemos recurrir a unidades extraíbles (USB, DVD, CD-R o CDRW) o al almacenamiento en la nube.

Otra opción es trabajar directamente en la nube con sus pros y sus contras:
Ventajas: No tendrás que estar almacenando las cosas regularmente pues dispone de autoguardado y sistema propio de Antivirus.
Desventajas: Requiere de conexión a Internet

Además, los sistemas operativos tienen la opción de programar puntos de restauración que nos permiten volver a tener nuestro PC como se encontraba en una fecha determinada.



> Algunas infecciones pueden deshabilitar la opción de restaurar el sistema del sistema operativo.

Mantente siempre actualizado

Parafraseando a Batman: "el mal no descansa", los hackers encuentran constantemente fallas de seguridad o hacen "mutar" a sus creaciones víricas. Es por esto que, los sistemas de seguridad deben estar siempre actualizados y, con esto, no nos referimos únicamente a los antivirus. Esto es aplicable también a todo el software que utilicemos con acceso a internet como navegadores y, sobre todo, nuestro sistema operativo.

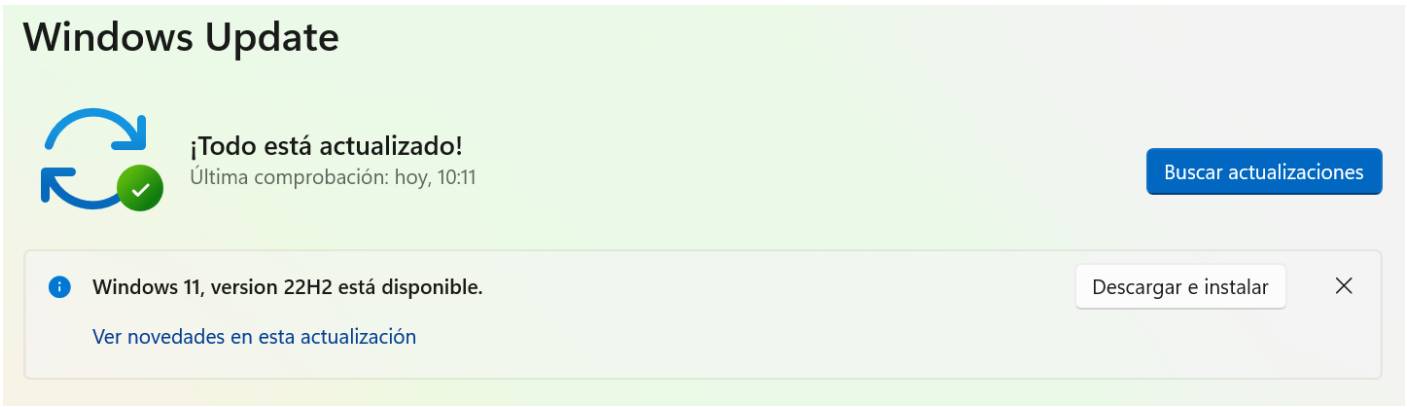


Ilustración: Buscar actualizaciones en Windows 11.

Utiliza distintas cuentas de usuario

El disponer de distintas cuentas de usuario y distintos permisos, también protegerá nuestros datos, sobre todo cuando utilicemos dispositivos compartidos.

Además de esto, las cuentas de un dispositivo pueden tener distintos roles y permisos:
Administrador: debe tener contraseña y ser la única con permisos para instalar aplicaciones, así como para configurar y actualizar el equipo.
Cuenta estándar: para el uso básico del equipo, pueden tener contraseña y se recomienda una por usuario que utilice el dispositivo regularmente. En ella pueden disponer de su configuración y sus carpetas de almacenamiento.
Cuenta invitado: para usuarios no habituales del equipo.

> Cuando estemos navegando en dispositivos que no son nuestros, es altamente recomendable utilizar el modo de incógnito, para no dejar datos de nuestra navegación tales como historial de navegación, contraseñas, caché...

Finalmente, hay cuentas reservadas a menores, o **herramientas de control parental** que pueden ser útiles para bloquear páginas y aplicaciones, limitar el tiempo de uso o generar informes de uso para los tutores de las criaturas.

El sentido común, el más común de los sentidos

Y es que no es más limpio el que más limpia, si no el que menos ensucia. Por mucho software de protección que tengamos, puntos de restauración o contraseñas seguras, si nuestro comportamiento no es prudente estaremos condenados a una infección. A continuación, vamos a dar una serie de consejos a tener en cuenta:

1. **Desconfía de mensajes y correos de remitentes desconocidos.** Estos pueden tener invitaciones u ofertas dudosas. En ocasiones presentan incongruencias gramaticales por estar traducidos automáticamente.
2. **No compartas datos personales ni sensibles** con remitentes desconocidos.
3. **Evita las cadenas de mensajes**, ya que además de tener un contenido más que cuestionable, son repositorios de direcciones que pueden utilizarse con otros fines.
4. **Evita utilizar redes Wi-Fi públicas abiertas**: ya que estas son utilizadas por hackers para acceder a información de aquellos que se conectan.

Amenazas Internas

> *Conoce a tu enemigo y conócete a ti mismo, y saldrás triunfador en mil batallas.*" Sun-Tzu, el Arte de la Guerra

Como ya hemos visto, las redes están llenas de potenciales peligros y amenazas externas pero, ¿qué pasa cuando la amenaza no es externa? A continuación vamos a ver los peligros de la adicción a Internet y los riesgos que conlleva para nuestra salud y bienestar digital.

Uso y consumo de tecnologías digitales

Este punto es muy importante, ya que **está directamente relacionado con nuestra salud.** El uso cada día más asiduo de las redes para la gestión prácticamente de cualquier cosa, hace que **a lo largo del día repitamos movimientos de forma continua** y mantengamos una **postura ergonómica relacionada con el dispositivo que usamos**. Esto significa que que **si el movimiento que repetimos es forzoso, a lo largo de los días desarrollemos una lesión** y acaba por condicionar nuestro estado de ánimo en el trabajo.

Es por ello que hay que **tener en cuenta los siguientes aspectos para tener** un uso sano de las tecnologías:

- **Aspecto postural**. Destacando la postura de la zona cervical y dorsal de la columna vertebral.
- **Aspecto visual**. En el que se destaca el uso prematuro de procedimientos de corrección de la graduación visual del menor por el uso de dispositivos digitales.
- **Aspecto mental**. Éste último es el que más preocupación produce en la sociedad actual, destacando:
  - El uso excesivo de dispositivos digitales, ya que el fin último es el consumo máximo de publicidad personalizada o encubierta por medio de influencers, la segmentación de perfiles para realizar acciones de marketing.
  - El ciberacoso o “bullying”, en el que se incluyen la difusión o recepción de bulos o fraudes que provocan desinformación o alarma social, el consumo o generación de discursos de odio, irrespetuosos o agresivos que pueden promover ideas extremistas, generando actitudes intolerantes o violentas y la pertenencia a comunidades que promueven conductas dañinas, trastornos alimenticios, autolesiones o consumo de drogas.

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

Youtube. Tu vida en las RRSS tiene público. Orange España

Adicción a la tecnología

Como ya hemos visto, las tecnologías digitales han venido para facilitarnos la vida, pudiendo ser de gran ayuda tanto en nuestro entorno laboral como en nuestro ocio. No obstante, su uso excesivo puede suponer un gran problema de salud y bienestar.

Las adicciones, hoy en día, suponen un gran problema de salud y no todas tienen por que ser a sustancias. El DSM-V, (manual de diagnóstico de trastornos mentales) ya ha incluido una sección de "Adicciones no relacionadas a sustancias", así como la OMS, que ya reconoce en su clasificación Internacional de Enfermedades (CIE) el "trastorno por videojuegos".

Señales de Alarma o Red Flags

Cuando una de estas adicciones se presenta, la persona adicta en cuestión puede presentar síntomas a los que hemos de prestar atención como:

- Uso excesivo de las TIC, llegando a perder la noción del tiempo.
- Empeoramiento del rendimiento laboral/escolar
- Apatía hacia otro tipo de actividades.
- Aislamiento social.
- Ansiedad cuando no se están utilizando tecnologías digitales.
- Salud descuidada (sueño, alimentación).
- Síndrome de abstinencia (irritabilidad al no utilizar las tecnologías digitales)

Consecuencias de la adicción a la tecnología

La adicción a las tecnologías digitales, como cualquier otra adicción, supone consecuencias en los planos social, psicológico, y físico.

En el **plano psicológico** se produce una gran inestabilidad emocional, con estados que pueden pasar de la depresión a la agresividad.

En el **plano social** encontramos las siguientes consecuencias: aislamiento social o limitando las relaciones personales a aquellas relacionadas con la adicción, falta de sinceridad con amigos y familiares, no cumplir objetivos ya sean domésticos, laborales o escolares.

En cuanto al **plano fisiológico** encontramos fatiga ocular por el uso de pantallas, fatiga mental y dolores de cabeza por el constante flujo de información así como cansancio y obesidad como consecuencia de un gran número de horas realizando esta actividad sedentaria. Además, los ciclos de sueño se ven alterados, produciendo irritabilidad e, incluso, alteraciones inmunitarias.

> Este es un contenido extensible al módulo 6 dada la vulnerabilidad del alumnado a las tecnologías digitales. Para obtener más recursos para trabajar en el aula visita: tudecideseninternet.es , portal para los más jóvenes de la Agencia Española de Protección de Datos (AEPD) donde encontrarás videos como el siguiente, para trabajar en el aula:

https://www.youtube.com/embed/tLYumn3qo5g

Youtube. UN CRACK DEL BMX (Versión larga). Agencia Española de Protección de Datos.

Adicción al móvil

También conocida como **nomofobia** (*del inglés NO-MObile-phone phobia)* hace referencia a la fobia irracional a no disponer del teléfono móvil físicamente o disponer de él pero sin sus funcionalidades (batería, cobertura), imposibilitando el acceso a la información y actualizaciones que este nos ofrece en redes sociales o servicios de mensajería. Este se enmarcaría dentro de la adicción a la tecnología y sus consecuencias son muy similares: irascibilidad, ansiedad y estrés.

Hemos de prestar atención a las siguientes **señales de alerta** para empezar a plantearnos si una persona tiene adicción al móvil.

- Más interacciones virtuales que reales (Whatsapp, RRSS...)
- El dispositivo es lo primero y lo último que atiendo cada día.
- Angustia, ansiedad e irritabilidad cuando no se puede disponer de las prestaciones del móvil (olvidado, sin batería o sin cobertura).

> SI quieres saber algunos tips de aplicaciones que nos ayudan a controlar nuestro tiempo, mira este vídeo en clave de humor sobre la adicción a los dispositivos:

https://www.youtube.com/embed/3khh4fiA6Xs

Adicción a los videojuegos

Práctica y uso excesivo y compulsivo de los videojuegos. Como todas las actividades, comienza a ser considerada adicción cuando afecta a los hábitos fundamentales del individuo en su día a día.

Como la adicción a la tecnología, interfiere en nuestra vida afectando al espacio y al tiempo dedicado a estas, dañando nuestras interaccione sociales y afectando a nuestra salud física y mental.

Además, los videojuegos, se basan en principios propios de la ludopatía clásica, que los hacen más adictivos como el feedback inmediato, haciendo que el cerebro genere dopamina, sensación placentera.

También se desarrollan en escenarios fantásticos alejados de la realidad.

Derecho a la desconexión digital

Los dispositivos digitales con conexión a internet, han supuesto una gran ayuda en el mundo laboral facilitando opciones como el **teletrabajo,** concepto que empezó a cobrar fuerza durante el primer año de la pandemia por COVID-19 en nuestro país.

Algo tan novedoso, albergaba muchos pros y contras, y entre ellos estaba un elemento que desconocíamos: la desconexión digital.

El hecho de estar confinados y sin un horario establecido de trabajo, hizo que este se extendiera a lo largo de toda la jornada (24 horas), lo que, a la larga, generó situaciones de estrés y ansiedad. No obstante, esta situación ya había sido contemplada en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales:

> **Artículo 88. Derecho a la desconexión digital en el ámbito laboral.**
>
> 1. Los trabajadores y los empleados públicos tendrán derecho a la desconexión digital a fin de garantizar, fuera del tiempo de trabajo legal o convencionalmente establecido, el respeto de su tiempo de descanso, permisos y vacaciones, así como de su intimidad personal y familiar."

¿Cómo conseguirlo?

Hay varios tips y herramientas que nos ayudarán a conseguir este propósito (que a veces se vuelve bastante dificil):

1. **Establece y delimita tu horario laboral,** fuera de este, no deberías prestar atención a e-mails o llamadas laborales.
2. Establece **canales para URGENCIAS** de tipo laboral, y lo de urgencias lo escribimos así con mayúsculas, no para cualquier actividad.
3. Aunque ya has establecido un horario laboral, estaría bien que te obligues a tener **periodos sin dispositivos tecnológicos** (PC o smartphone) así como socializar con los tuyos.
4. Utiliza las facilidades que te ofrecen los dispositivos: **Modo no molestar, horario de notificaciones.**.. Para esto, aunque muchos terminales ya disponen de su propio configurador de horario, han surgido distintas apps como OFFTIME, que permite **bloquear un buen número de aplicaciones o llamadas entrantes** que sepas que te pueden

molestar o incluso establecer un horario de bloqueo. Puedes conocer más apps para la desconexión digital pulsando aquí.

5. **Separa tu vida laboral de tu vida personal**: Procura no utilizar cuentas personales para asuntos laborales.

Amenazas Externas

Phishing, qué es y cómo evitarlo

> El **phishing es una de las estafas con mayor trayectoria** y mejor conocidas de Internet. Es un tipo de fraude que se da en las telecomunicaciones y que emplea trucos de ingeniería social para obtener datos privados de sus víctimas. La diferencia entre Spam y Phishing es clara: el Spam es correo basura, no es más que un montón de anuncios no deseados. **El phishing por otro lado, tiene como finalidad robar tus datos y utilizarlos contra ti.**

La **mayor parte del phishing puede dar como resultado el robo de identidades o de dinero, y también es una técnica eficaz para el espionaje industrial y el robo de datos**. “Algunos hackers llegan incluso a crear perfiles falsos en redes sociales, invierten un tiempo en desarrollar una relación con las posibles víctimas y esperan a que exista confianza para hacer saltar la trampa”.

Un ataque de phishing tiene 3 componentes:

1. El ataque **se realiza mediante comunicaciones electrónicas, como un correo electrónico, un SMS o una llamada de teléfono.**
2. El atacante **se hace pasar por una persona u organización** de confianza.
3. El **objetivo es obtener información personal confidencial**, como credenciales de inicio de sesión o números de tarjeta de crédito.

> Como a veces es difícil detectarlo, aquí te dejamos una serie de **características y trucos que pueden funcionar** para **detectar** un intento de **phishing:**

- Sé **precavido ante los correos** que aparentan ser de entidades bancarias o servicios conocidos (Dropbox, Facebook, Google Drive, Apple ID, Correos y Telégrafos, Agencia Tributaria, etc.) con mensajes que no esperabas, que son alarmistas o extraños.
- **Sospecha si hay errores gramaticales en el texto,** pueden haber utilizado un traductor automático para la redacción del mensaje trampa. Ningún servicio con cierta reputación enviará mensajes mal redactados.
- Si recibes **comunicaciones anónimas del tipo “Estimado cliente”, “Notificación a usuario” o “Querido amigo”,** es un indicio que te debe poner en alerta.
- **Si el mensaje te obliga a tomar una decisión de manera inminente o en unas pocas horas, es mala seña**l. Contrasta directamente si la urgencia es real o no directamente con el servicio o consultando otras fuentes de información de confianza: la OSI, Policía, Guardia Civil, etc.

- **Revisa si el texto del enlace que facilitan en el mensaje coincide con la dirección a la que apunta,** y que ésta corresponda con la URL del servicio legítimo.
- **Un servicio con cierto prestigio utilizará sus propios dominios para las direcciones de email corporativas**. Si recibes la comunicación desde un buzón de correo tipo @gmail.com, @outlook.com o cualquier otro similar, sospecha.
- Aplica la **ecuación: solicitud de datos bancarios + datos personales** = fraude.

Ciberacoso

UNICEF lo define como:

> Ciberacoso es acoso o intimidación por medio de las tecnologías digitales. Puede ocurrir en las redes sociales, las plataformas de mensajería, las plataformas de juegos y los teléfonos móviles. Es un comportamiento que se repite y que busca atemorizar, enfadar o humillar a otras personas.
>
> - **Difundir mentiras o publicar fotografías** o videos vergonzosos de alguien en las redes sociales.
> - **Enviar mensajes, imágenes o videos hirientes**, abusivos o amenazantes a través de plataformas de mensajería
> - **Hacerse pasar por otra persona** y enviar mensajes agresivos en nombre de dicha persona o a través de cuentas falsas.

Y por último, en el caso de que nuestro alumnado reciba el tan temido ciberacoso hay que enseñarles a gestionarlo:

- En un primer momento hay que **crear un clima de confianza con el menor** en el que entienda que se le escucha y se le apoya, evitando culpabilizar a nadie.
- Hay que **guardar evidencias** de la situación generada mediante capturas de pantalla de los mensajes, fotografías o vídeos.
- **Contactar con las Fuerzas y Cuerpos de Seguridad** en caso de reiteración, gravedad o ilegalidad del comportamiento.

IS4K de INCIBE. Ciberacoso escolar.

> INCIBE es el Instituto Nacional de Ciberseguridad y tiene una web específica para el uso seguro en menores (IS4K). En ella se puede obtener más información sobre ciberacoso escolar en el siguiente enlace.

Sexting

Etimológicamente proviene de los anglicismos SEX (sexo) y TEXTING (mensajería de texto) y hace referencia a la producción y difusión de contenido sexual mediante aplicaciones de mensajería digital.

Estudios nacionales afirma que el 31% de los menores de entre 11 y 16 años ha recibido ha recibido mensajes sexuales de algún tipo principalmente por servicios de mensajería instantánea, habiendo aumentado exponencialmente frente al 10% del año 2010.
Entre sus características encontramos:

- Uso de medios digitales para la producción.
- Contenido erótico/sexual
- Protagonistas identificables en el contenido difundido.
- Naturaleza privada en su origen.

Pero pese a ser contenidos privados, pueden ser difundidos debido a:

- Pérdida del dispositivo
- Fallo de seguridad
- Haber sido enviado a un destinatario erróneo
- O difusión posterior por parte del receptor del mensaje sin estar autorizado.

Esto puede acarrear consecuencias como:

- **Sextorsión**: Utilización de material privado de contenido sexual para chantajear.
- **Ciberbulling o Ciberacoso**
- **Grooming**: Forma de acoso en la que un adulto contacta con un menor con el fín de ganarse su confianza para posteriormente involucrarle en una actividad sexual.
- **Pornovenganza**: difusión de contenido íntimo en redes sociales o servicios de mensajería sin consentimiento del protagonista.

Todas estas actuaciones conllevarán a la exigencia de
-**Responsabilidad en materia de protección de datos** por difusión de datos sensibles sin consentimiento.
-**Responsabilidad civil**: por daños y perjuicios materiales y morales, con su consecuente sanción administrativa e indemnización
-Responsabilidad penal: la grabación y difusión de imágenes o vídeos sin consentimiento podrá ser constitutiva de delito, sancionable con penas de hasta 5 años de prisión. Y de **uno a tres meses para quienes difundan, revelen o cedan a terceros sin consentimiento de la víctima**.

https://www.youtube.com/embed/s_O1FlEc1xk

Youtube. No puedes compartirlas sin su consentimiento #RevengePorn. Pantallas Amigas

> Para saber más, échale un ojo al libro de "*Convivencia segura en la red, ciberayudantes*"