2º de Bachillerato

Tecnologías de la Información y Comunicación

Contenidos

Políticas de protección de datos: Seguridad en redes sociales

¿Quién no usa hoy en día Facebook? ¿o quién no habla por WhatsApp? ¿o quién no tiene cuenta en Google?

Las redes sociales, son sin lugar a duda, una potente herramienta que nos permite compartir nuestros gustos, aficiones, fotos, recuerdos, opiniones, etc. con otras personas. A través de ellas podemos ampliar nuestro círculo de amistades, nuestras relaciones personales y profesionales, acceder a grupos con los mismo intereses, etc.

Pero ..¿es todo tan bueno como parece? La respuesta es no. Las redes sociales, son al fin y al cabo un almacén, externo a nosotros, con muchos de nuestros datos personales, que pueden ser accedidos por terceros con no tan buenas intenciones.

Veremos en este tema como podemos cuidar de esos datos de forma que sólo se compartan con las personas adecuadas, cuáles son los datos que nunca debemos publicar y qué medidas de seguridad debemos adoptar para proteger nuestra identidad digital.

Debemos ser conscientes de la cantidad ingente de datos que ofrecemos en internet, en las redes sociales, en nuestras búsquedas en google, desde el móvil...

Es nuestra obligación hacernos responsables de esos datos, proteger a la infancia, y seguir una serie de medidas que propicien la seguridad y privacidad de nuestros datos:

https://www.youtube.com/embed/WqBl2zyXI7g?rel=0

Campaña de Unicef Redes. Lo que la red sabe de ti

Importante

Una **red social** es una forma de interacción social basada en el intercambio dinámico entre personas, grupos e instituciones. Son sistemas abiertos y en permanente construcción en los que se forman grupos en torno a un tema común.

Desde el momento en que nos damos de alta en una red social, facilitamos una serie de datos personales o profesionales que quedarán en los servidores de la red social (aún después de borrarla) y que pueden ser accedidos por personas que hagan un mal uso de estos datos, difundiéndolos o usándolos para fines poco éticos o ilegales.

Debes ser muy estricto en la información que compartes, ya que aunque tengas configurado los permisos de acceso a tu perfil, puede ser que algunos datos o fotos sean accedidos a través de amigos de amigos al comentar alguna de nuestras publicaciones o poner un "like".

Imagen en Pixabay de Geraltbajo licencia CCO Public Domain

Importante

Cuando te des de alta en redes sociales valora qué información es la que quieres proporcionar.

Y tanto en los datos de tu perfil como en lo que publicas, se precavido y no compartas nunca información que pueda comprometer tu privacidad:

- Datos personales
- DNI o pasaporte
- Contraseñas
- Teléfono
- Correo electrónico
- Dirección donde vives
- Lugar de trabajo
- Ubicación
- Fotos o vídeos comprometidas
- Planes para las vacaciones
- Ideología
- Creencias

Y por supuesto verifica tu configuración de la privacidad para controlar quién puede acceder a tus datos.

Para saber más

1.1. Alta o acceso: verificación en dos pasos

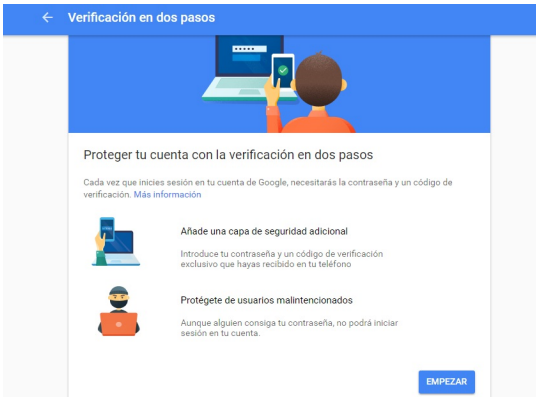

Imagen de creación propia bajo licencia CC

La verificación en dos pasos en un mecanismo de seguridad que añade una capa de protección adicional al acceso por contraseña.

Por ejemplo, cuando nos damos de alta en algún servicio web, a la hora de registrarnos, solemos facilitar nuestro correo y una contraseña, sin embargo nuestra cuenta no estará activa hasta que vayamos a un mensaje que habremos recibido en nuestro correo y hagamos click en un enlace que se nos envía. Con esto el servicio se asegura de que realmente eres el propietario de la cuenta de correo que estás facilitando.

Algo parecido ocurre cuando hacemos alguna transacción desde nuestra página de banca online (al menos en la mayoría), no solo nos pide la clave de operaciones sino que además nos pide un código de verificación que se nos envía al móvil, así no solo deberemos tener los datos de acceso a la página, si no también el código para operaciones y además tener acceso al móvil asociado a nuestro usuario. Con lo que la seguridad se refuerza.

Google ha incorporado también este mecanismo adicional de seguridad para acceder a nuestra cuenta. Esta opción, una vez que se activa (desde el menú de configuración) nos pedirá cada vez que vayamos a acceder, además de nuestra contraseña, un código que se nos envía al móvil. Una vez que hemos accedido por ejemplo a nuestro ordenador, podemos desactivarlo para ese dispositivo, para que no nos lo pida más, pero dejarlo activo para otros para los que no tengamos tanta seguridad de que somos los únicos que los usan.

VERIFICACIÓN EN DOS PASOS DE GOOGLE

Desde tu gmail o google, si haces click en el icono de tu perfil que aparece arriba a la derecha, y pulsas en "Mi cuenta" podrás acceder a distintas opciones de configuración de tu cuenta. Entre ellas, la verificación en dos pasos para acceder a tu cuenta:

Gestionar tu cuenta de Google / Seguridad / Cómo inicias sesión en Google / Verificación en dos pasos

Facilitarás un número de teléfono al que se te enviará un código (vía mensaje, llamada o a través de la aplicación móvil) cuando vayas a logearte en tu cuenta. De esta manera necesitas estar en posesión de la clave de acceso mas el móvil al que recibes el código de verificación.

Sí quieres saber más de esta interesante opción aquí te lo explicamos.

1.2. Tu privacidad

Es fundamental revisar las opciones de configuración que nos ofrecen las distintas aplicaciones y redes sociales para controlar quién tiene acceso a nuestros datos y qué puede hacer con ellos.

Ante la duda, selecciona siempre las opciones más restrictivas.

Selecciona muy bien a quién permites acceso, no confíes en nadie que no conozcas lo suficientemente bien, aún así cabe el riesgo de que alguien suplante la identidad de algún amigo tuyo sin que lo sepas y tenga acceso a tus datos, por lo que si ves cualquier cosa extraña en los comentarios o acciones de un amigo, intenta verificar que realmente es él

Imagen de creación propia bajo licencia CC

1.3. Permisos a aplicaciones

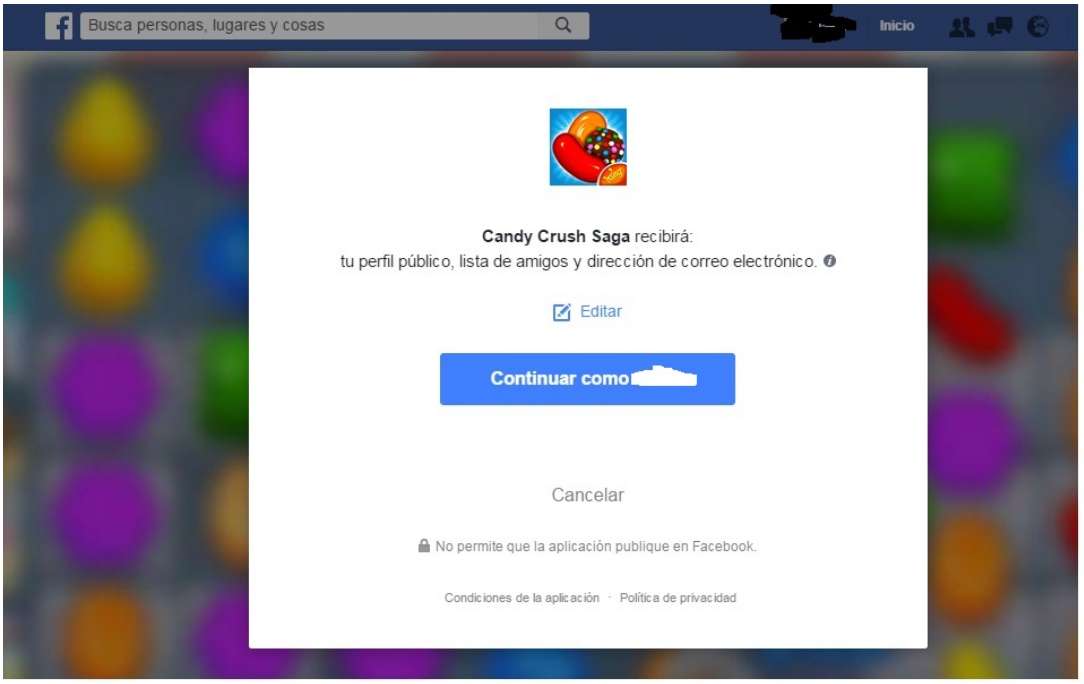

Imagen de creación propia bajo licencia CC

Desde las redes sociales tenemos acceso a multitud de juegos (CandyCrash, Farmville..) o aplicaciones.

Muchas veces es posible que nos lleguen peticiones de un juego a través de un amigo y esto es porque la aplicación, simplemente por usarla o jugar, toma ciertos datos de tu perfil, entre ellos posiblemente, tu lista de amigos. Por ello, es muy importante que antes de instalar cualquier aplicación que se nos sugiera o de jugar, leamos atentamente las condiciones de uso o de privacidad.

Algunas veces estas condiciones se nos muestran claramente junto al botón de jugar, pero otras aparece en alguna sección más escondida. Los juegos pueden acceder entre otros a:

- Tu nombre
- Foto de perfil
- Lista de amigos
- Correo electrónico
- Género
- Fecha de nacimiento
- Actividad
- Localización

Information We Collect and How We Collect It

Information About You That We Get From Connected Third-Party Applications, Including Social Networks (like Facebook)

If you play Zynga's games or access any of our other Services on connected third-party applications or connect our Services to any third-party applications, including social networks like Facebook, Zynga may receive certain information about you from the provider of the third-party application. The information we receive depends on the Zynga game you're playing, the third-party application, your privacy settings and, if applicable, your friends' privacy settings on that third-party application.

For example, Zynga may collect and store some or all of the following information shared by the provider of the connected third-party application:

- your first and last name;
- your profile picture or its URL;
- your user ID number (like your Facebook ID number), which may be linked to publicly-available information like your name and profile photo;
- the user ID number and other public data for your friends;
- the login e-mail you provided to that third-party application when you registered with it;
- your physical location and that of the devices you use to access our Services;
- your gender;
- your birthday and/or age range;
- information about your activities on or through the connected third-party application;
- other publicly-available information on the third-party application; and/or
- any other information that you or the provider of the third-party application share with Zynga.

If you access our Services from a third-party application or connect our Services to a third-party application, you should also read that third-party application's Terms of Service and Privacy Policy.

If you are unclear about what information a third-party application is sharing with us, please go to the third-party application to find out more about their privacy practices.

Cookies and Automated Information Collection

We and service providers acting on our behalf, like Google Analytics, store log files and use tracking technologies such as:

Imagen de creación propia bajo licencia CC

1.4. Suplantación de identidad

En las redes sociales o, en internet en general, existen dos formas de hacerse pasar por nosotros, tanto para acceder a todos nuestros datos personales como para publicar lo que quieran con nuestra propia identidad digital:

- **Robo de identidad a través del Phising:** robo de nuestro usuario y clave y acceso a nuestro ordenador y nuestras redes para fines fraudulentos. Normalmente se produce a través del correo electrónico o mensajería, el usuario recibe un mensaje con apariencia oficial donde el cibercriminal requiere los datos personales suplantando una imagen corporativa (un banco, una página de recarga de móviles,...).
- **Suplantación de identidad**: alguien crea una cuenta con un nombre muy parecido a la nuestra, probablemente usando alguna de nuestras fotos y con nuestros datos, de forma que se hace pasar por nosotros, aceptando solicitudes de nuestros amigos que por confusión lo agregan.

Ambos métodos pueden ser usados con fines poco éticos o incluso ilegales.

Si crees que has sufrido algún posible robo o suplantación de tu identidad digital, puedes denunciarlo desde la página de Delitos Telemáticos de la Guardia Civil.

Para prevenir el phishing podemos seguir los consejos de la Asociación de Internautas.

Imagen de Policia Nacional en Wikimedia. Licencia CC

1.5. CiberAcoso

A través de las redes sociales podemos ser víctimas de acoso, podemos recibir insultos, amenazas de publicación de fotos o datos personales comprometidos, chantajes, etc.

Por todo esto debemos ser muy cuidadosos a la hora de permitir acceso a datos comprometidos, es más, estos jamás deberíamos publicarlos en redes sociales por muy bien configuradas que tengamos nuestras restricciones de acceso y privacidad.

Si sufrimos algún ataque de este tipo debemos, en primer lugar bloquear al atacante y luego denunciar, para la denuncia es importante que captures todos los pantallazos necesarios donde aparezcan las amenazas o cualquier otro signo de acoso, así como guardar (no borrar) los mensajes o imágenes que te envíe.

Para denunciar puedes hacerlo a través de la página del Grupo de Delitos Telemáticos de la Guardia Civil, aunque para completarla deberás personarte en algún centro policial o judicial.

Cyberbulling o Ciberacoso:

Este término se refiere al acoso entre iguales a través de las redes sociales.

Estamos ante un caso de **ciberbullying** cuando un o una menor atormenta, amenaza, hostiga, humilla o molesta a otro/a mediante Internet, teléfonos móviles, consolas de juegos u otras tecnologías telemáticas.

https://www.youtube.com/embed/SEC_dOWFN5M?rel=0

Vídeo de PantallasAmigas. Ciberbullying: ciberacoso en redes sociales

Grooming: En este caso, el acoso se realiza por parte de un adulto que engatusa a algún menor, bien haciéndose pasar por otro menor, ofreciendo regalos, etc.

En la mayoría de los casos, el adulto aprovecha su posición de poder para chantajear al menor a cambio de favores sexuales.

Sexting: Exhibicionismo online, fenómeno por el que jóvenes o adolescentes intercambian mensajes, fotos o vídeos eróticos o de desnudos. El problema surge con la difusión de estás imágenes fuera del contexto de privacidad, por lo que el remitente inicial pierde todo el control de sus imágenes, facilitando un posterior uso de las mismas por parte de terceros.

Para prevenir y no caer en estos riesgos, téngase en cuenta los consejos de este Decálogo contra el grooming y el acoso sexual en las redes.

Curiosidad

Un caso de ciberacoso: conozcamos de primera mano el acoso que los famosos pueden llegar a recibir en las redes sociales con el visionado del programa Salvados de Jordi Évole.

http://www.lasexta.com/embed/el-sufrimiento-de-paula-vazquez-al-ser-insultada-en-redes-sociales-les-pegaria-un-cabezazo-y-les-romperia-la-nariz-pero-al-final-no-lo-hago-y-denuncio/video/7/2018/02/18/5a89d06a7ed1a8040881ed81

Vídeo de La Sexta TV. El sufrimiento de Paula Vázquez al ser insultada en redes

1.6. Credibilidad de la información

La carencia de control sobre la publicación de información en la red, la facilidad de piratería o sabotaje electrónico y la facilidad de alteración del contenido, son algunas de las características que hacen que los contenidos web deban ser seleccionados.

La mayoría de las publicaciones web se hacen en sitios que no tienen ninguna política editorial explícita acerca de la revisión de documentos y también es muy común la falta de identificación del autor o de su profesión.

Importante

Una buena forma de comprobar la credibilidad de la información que estamos buscando es revisar los siguientes puntos:

1. **Presentación.-** nombre del sitio o título de la página, detaller de la URL, tipo de dominio (edu, org, com), tipo de publicación (educativa, comercial, informativa).
2. **Autoría.-** es identificable, indica datos sobre la biografía profesional del autor o autora, aparecen sus datos de contacto.
3. **Destinatario.-** estilo de la página, enfoque con el que se presenta, a quién está dirigida (alumnado, académicos, compradores, público en general).
4. **Precisión.-** se indican las fuentes de información, se incluyen sistemas de verificación, los enlaces a otros sitios son adecuados, la información está organizada.
5. **Actualidad.-** existe un mantenimiento del sitio, la información se actualiza periódicamente.

Cuando se requiera una información, es preciso tener en cuenta algunas marcas que nos van a permitir **evaluar la confianza y veracidad** de ese sitio. Algunas de ellas son:

- Información obtenida de instituciones.- los sitios web de instituciones tales como organismos públicos, universidades, asociaciones de profesionales, etc, deben ser los primeros lugares en los que buscar información creíble.
- Links recomendados por sitios institucionales.- en los sitios web de instituciones suelen recomendar otras páginas o sitios que han sido validados y que ofrecen más contenidos sobre la información en cuestión.
- Información actualizada.- es importante conocer la fecha de publicación de la información ya que muchas veces ésta ha caducado o ha sido superada. En algunos sitios web, la fecha de actualización se encuentra al final de la página o en un lateral y en otros ni siquiera es explícita y hay que rastrearla.

A título personal puedes hacer:

- Comparar la noticia en diferentes medios o fuentes de información.
- No quedarte en el titular de la noticia, leerla completamente y, si es posible, visualizar completos los vídeos originales.
- Preguntarte por la fecha y el contexto de la noticia.
- Evitar los clickbait (ciberanzuelos) y no ller ni dinfundir fake news (noticias falsas).

2. Facebook

Imagen en Wikimedia Commons bajo licencia Public Domain

Facebook es sin duda una de las redes sociales más populares, con 1.650 millones de usuarios activos (dato del 27 de abril del 2016).

Esta red social nos ofrece una configuración de privacidad bastante detallada, con muchas posibilidades, desde el menú **Configuración /Privacidad,** aunque muchas veces por ignorancia o dejadez se dejan los valores por defecto. Es importante revisar esta configuración. A continuación veremos algunos de los aspectos más importantes a revisar.

- **Publicaciones**: para cada actualización de estado, foto o vídeo que publiques puedes decidir quién puede verla. Desde el menú superior derecho de la publicación dirás si quieres que sea pública (en cuyo caso la podrá ver todo el mundo), si la deseas compartir solo con amigos, o con grupos específicos de personas.
- **Perfil**: para saber cómo ven los demás tu perfil, tienes la opción de "ver como..". Accede a esta opción desde los tres puntos que aparecen al pie de tu foto de portada. Podrás seleccionar ver como "Público" o ver como alguno de tus amigos en concreto. Así sabrás si todo está correctamente configurado.
- **Lista de amigos**: Desde inicio, en el menú izquierdo podrás acceder a "lista de amigos" y crear listas añadiendo o quitando a los amigos que desees. Estas listas las usarás después para para controlar quién ve tus publicaciones.
- **Comentarios y me gusta:** Todos los autorizados a ver tu publicación podrán ver comentarios, comentarla y poner me gusta. Si no deseas que ciertas personas tengan acceso, puedes modificar el público con el que compartes esa publicación.
- **Etiquetas**: Cuando etiquetas a alguien en una foto, esa persona y sus amigos podrán ver la foto, para evitarlo abre la foto y cambia el público con el que la compartes, eliminando "amigos de la persona etiqueta". Para gestionar cómo aparecen las fotos en las que otros te etiquetan vete al menú Biografía y etiquetado, desde allí podrás decidir si quieres aprobar las etiquetas antes de que se publiquen, si quieres que se vea en tu muro, etc..
- **Desactivación y eliminación de la cuenta**: es posible desactivar tu cuenta si lo deseas, deshabilitándose (no borrándose) la mayoría de los datos que hayas publicado, aunque algunos contenidos que hayas intercambiado con amigos seguirás estando visibles. En caso de que lo desees, podrás reactivar tu cuenta sin más que acceder a ella. Si lo deseas también puedes eliminar tu cuenta definitivamente.

Reflexiona

¿Cómo ve cualquier extraño nuestro perfil de Facebook? ¿qué información tiene accesible?

Para ver tu perfil de Facebook como alguién concreto o como cualquier persona que no esté entre tus amigos ("Público"):

https://www.facebook.com/help/288066747875915?helpref=faq_content

Mostrar retroalimentación

¿Has comprobado que ve exclusivamente lo que debería? ¿que quedan ocultos todos los datos, fotos e información personal?. Si no es así, debes revisar la configuración de tu privacidad.

Curiosidad

En los primeros meses de 2018 saltó la noticia, los datos personales de millones de perfiles de Facebook, la red social más extendida en el mundo, han sido utilizados con fines comerciales sin

Cambridge Analytica y la MAYOR POLÉMICA de Facebook en su historia

Para profundizar en el tema, lee la siguiente noticia publicada en el portal de noticias tecnológicas Xataka:

¿Qué ha pasado con Facebook?

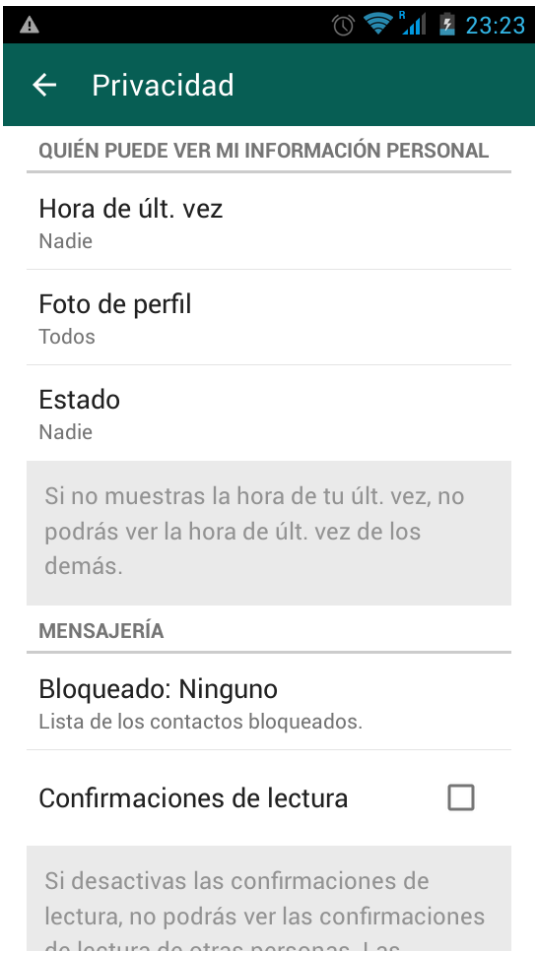

Imagen de creación propia bajo licencia CC

Desde el menú de **Configuración/Ajustes/Cuenta/ Privacidad** podrás configurar distintas opciones como:

- quién puede ver tu foto de perfil y estado
- quién puede ver tu hora de última conexión. Si pones nadie, tú tampoco podrás ver la fecha de última conexión de tus contactos. Bastante justo ¿no?.
- quitar el doble check azul de confirmación de lectura. Al igual que con la hora de última conexión, si deshabilitas las confirmaciones de lectura, tampoco verás las de tus contactos.
- bloquear contactos. Las personas bloqueadas no nos podrás mandar mensajes.

Curiosidad

CIFRADO DE LAS CONVERSACIONES DE WHATSAPP

Whatsapp ha incorporado el cifrado de sus conversaciones extremo a extremos, de forma que solo emisor y receptor dispondrán de las claves de descifrado, de forma que si alguién o el mismo whatsapp intercepta una conversación cifrada, no tendrá acceso al contenido.

Para saber más haz click aquí

4. Google

¿Qué sabe Google de nosotros?, pues mucho. Este gigante informático controla multitud de aplicaciones que usamos a diario (Youtube, Gmail, Drive, Google Maps, búsquedas en Google, Google+, etc.), y a través de ellas puede conocer nuestro gustos, intereses o dónde nos movemos y enviarnos publicidad asociada a estos intereses. Muchas veces esto puede ser útil para todos los participantes, nosotros, usuarios, recibimos ofertas y anuncios que nos interesan, las empresas hacen uso de una publicidad más personalizada y eficiente y Google estará también satisfecho porque anunciantes y usuarios hacen uso de sus servicios y plataformas. Sin embargo puede ser que a veces nos moleste este control excesivo de nuestra actividad y deseemos modificar estos parámetros.

Los principales enlaces desde los que consultar o modificar lo que Google sabe de tí son (todos estos enlaces son accesibles desde los servicios de Google, haciendo click en el icono que aparece arriba a la derecha y seleccionando **Cuenta**):

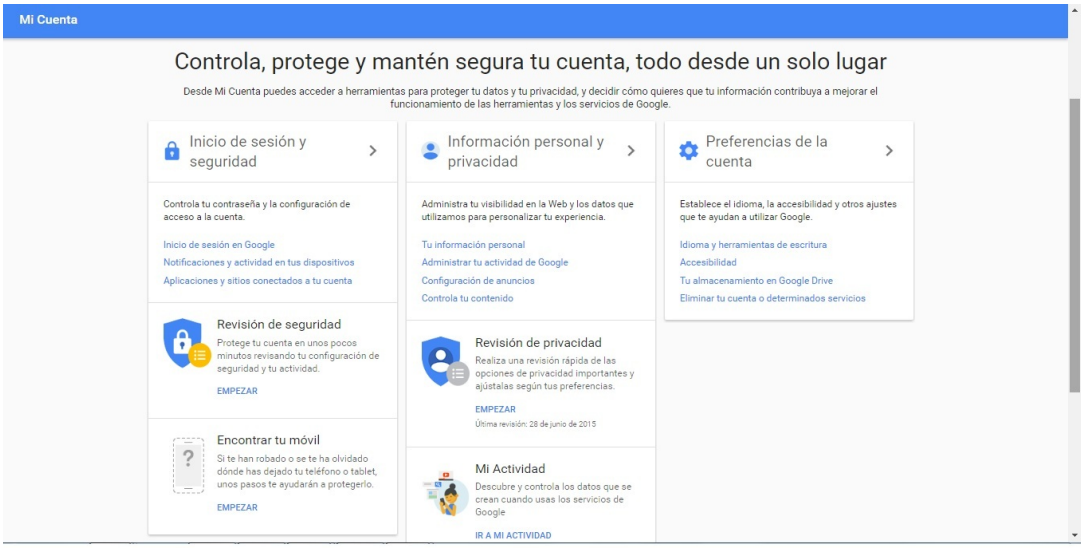

Imagen de creación propia bajo licencia CC

- **Publicidady anuncios que recibes**: https://www.google.com/settings/u/0/ads/authenticated
- **Ubicación y lugares en los que has estado**: https://www.google.com/maps/timeline
- **Historial de busquedas:** https://myactivity.google.com/myactivity
- **Historial de Youtube:** https://www.youtube.com/feed/history/search_history
- **Los dispositivos desde donde te conectas:** https://security.google.com/settings/security/activity
- **El software y aplicaciones que utilizas asociadas a tu cuenta:** https://security.google.com/settings/security/permissions
- **Exportar tus datos:** https://takeout.google.com/settings/takeout

Para saber más

En este vídeo podrás ver la explicación de las distintas posibilidades:

http://www.youtube.com/embed/aKnY9582Szc

Video en Youtube de sp26

5. Ley de Protección de Datos de Carácter Personal

El desarrollo e implantación de las TIC ha dado lugar a su presencia en casi todas las actividades sociales, culturales, empresariales.

Las TIC intervienen inevitablemente en la configuración de las relaciones que mantienen las empresas entre sí y con los particulares. La principal consecuencia es la necesidad de una mayor protección de los derechos y de los datos, garantizando la privacidad de las personas. *¿Quién no ha recibido una llamada a horas intempestivas ofreciéndole una conexión a Internet baratísima?*

Como respuesta a esta necesidad se promulgó la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y se creó la **Agencia Española de Protección de Datos,** cuya función principal es "velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos".

En caso de tener pruebas o indicios de que se haya incumplido la Ley Órganica de Protección de Datos, puedes denunciarlo, presentando las pruebas y datos oportunos, en la Agencia Española de Protección de Datos.

Importante

La Agencia Española de Protección de Datos es el organismo encargado de velar por los derechos de las personas físicas en relación a sus datos de carácter personal, tanto en cuanto a su recogida y almacenamiento como a su distribución y uso.

La ley que regula esto es la RGPD *(Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales basada en el Reglamento Europeo General de Protección de Datos)*, entendiéndose por datos de carácter personal tanto ficheros o bases de datos en soporte informático, como impresos, vídeos, audios, etc.

Reflexiona

Si lees la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, verás que hay sanciones asociadas a cada tipo de infracción, pudiendo llegar a ser bastante importantes para el caso de las infracciones muy graves.

Mostrar retroalimentación

Una infracción leve sería el obligar a nuestros clientes a rellenar una serie de datos al darse de alta, sin informarles del tratamiento que se va a dar a esos datos.

Una infracción grave sería el tratar datos de carácter personal sin el consentimiento de los afectados.

Sería una infracción muy grave el engañar a los usuarios diciéndoles que sus datos van a ser tratados para un determinado fin que es falso y usarlos para otro.

Curiosidad

HERRAMIENTAS DE CONTROL PARENTAL

Las herramientas de control parental pueden ser usadas por los padres para restringir el acceso de sus hijos a páginas o aplicaciones inapropiadas, o para cualquier cafetería, colegio, biblioteca, etc. con acceso a Internet, para evitar que niños o adultos accedan a ciertos contenidos o sitios no deseados. Algunos también incluyen restricciones de caracter temporal que limitan el acceso a un determinado horario.

Es posible la restricción por palabras, de forma que si el contenido al que se va a acceder contiene la palabra "prohibida" se cerrará la pestaña del navegador o la restricción por sitio, si el sitio de destino está en la lista de sitios no permitidos no se podrá acceder a él. Ambas listas, palabras y sitios deben irse actualizando.

Se pude trabajar con listas blancas o negras, las blancas permiten el acceso a lo que contienen (habría que cerrar el resto) y las negras indican donde no se puede acceder (el resto estaría permitido)

Imagen de creación propia bajo licencia CC

Para saber más

Te dejamos un programa de control parental gratuito (existen muchos otros):

GOLDEN FILTER PREMIUM

Descarga del producto
Documentación (en inglés)

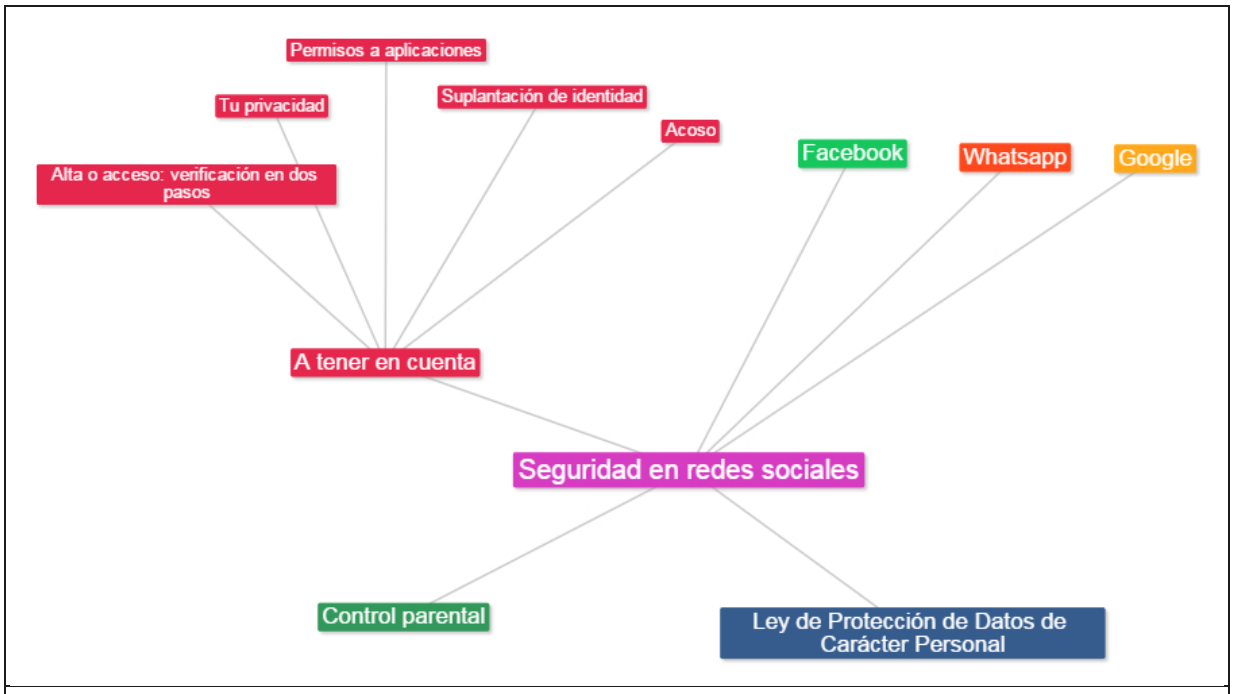

Imagen de creación propia bajo licencia CC

Aviso Legal

https://www.juntadeandalucia.es/educacion/permanente/materiales/index.php?aviso#space

2º de Bachillerato

Tecnologías de la Información y Comunicación

Contenidos

Políticas de protección de datos: Seguridad en redes sociales

¿Quién no usa hoy en día Facebook? ¿o quién no habla por WhatsApp? ¿o quién no tiene cuenta en Google?

Las redes sociales, son sin lugar a duda, una potente herramienta que nos permite compartir nuestros gustos, aficiones, fotos, recuerdos, opiniones, etc. con otras personas. A través de ellas podemos ampliar nuestro círculo de amistades, nuestras relaciones personales y profesionales, acceder a grupos con los mismo intereses, etc.

Pero ..¿es todo tan bueno como parece? La respuesta es no. Las redes sociales, son al fin y al cabo un almacén, externo a nosotros, con muchos de nuestros datos personales, que pueden ser accedidos por terceros con no tan buenas intenciones.

Veremos en este tema como podemos cuidar de esos datos de forma que sólo se compartan con las personas adecuadas, cuáles son los datos que nunca debemos publicar y qué medidas de seguridad debemos adoptar para proteger nuestra identidad digital.

Debemos ser conscientes de la cantidad ingente de datos que ofrecemos en internet, en las redes sociales, en nuestras búsquedas en google, desde el móvil...

Es nuestra obligación hacernos responsables de esos datos, proteger a la infancia, y seguir una serie de medidas que propicien la seguridad y privacidad de nuestros datos: