Guía para el docente

Nivel educativo: Secundaria

Objetivo de la sesión: Conocer qué es la huella digital y sus implicaciones en la vida cotidiana, a través de actividades dinámicas que permitan al alumno reflexionar sobre su importancia en la formación de nuestra identidad digital.

Tiempo: 120 min (en caso de contar con menos tiempo, queda a criterio del profesor omitir algunas de las actividades sugeridas).

Material:

-Pizarrón o rotafolio

-Computadora

-Proyector

-Presentación PowerPoint

-Infografías

-Video

-Sobres de un solo color (1 por alumno)

-Formato de red social

-Fotografías de personas o momentos más representativos de cada alumno y evidencias de información personal que sea de interés y defina su personalidad, por ejemplo: cartas, boletos, estampas, recortes, etc. (solicitarlo previamente a cada alumno)

-Pluma, lápiz y lápices de colores.

Descripción de la sesión:

1. El profesor(a) mediará una lluvia de ideas con el fin de conocer el conocimiento previo de los alumnos sobre el tema.

2. Se llevará a cabo la parte 1 de la actividad **"*Dime qué compartes y te diré quién eres*"**

3. El profesor(a) expondrá el tema apoyándose de la **presentación en PowerPoint**.

4. Dentro de la presentación de forma intercalada se presentarán las **infografías** a través de una breve dinámica. Para ello, antes de iniciar la sesión, el profesor deberá formar equipos (el número de integrantes depende del total de alumnos en el grupo y queda a consideración del profesor, se sugieren equipos de 3 a 5 alumnos) y escribirá en un papel el nombre de cada equipo.

5. Se llevará a cabo el cierre de la actividad **"*Dime qué compartes y te diré quién eres*"**

6. Se presentará el **video**.

7. Se llevará a cabo una dinámica final de reflexión sobre el tema.

Contenido de la sesión:

A continuación, se presenta información detallada sobre ***huella digital***, en la que se especifica en qué plantilla de la **presentación de Power point** se encuentra cada parte de la información.

Plantilla 1:

El profesor(a) pedirá a los alumnos que respondan a las siguientes preguntas:

¿Qué es la huella digital?, ¿Qué suponen o creen que es huella digital? o ¿Qué palabras vienen a su mente cuando escuchan huella digital?

El profesor o algún alumno que el maestro indique deberá anotar en el pizarrón o rotafolio, las palabras e ideas que los alumnos van mencionando, esto les permitirá tener una mejor visión del concepto previo que tengan los alumnos sobre este tema y todo lo que puede definir a la huella digital.

Al finalizar la lluvia de ideas deberán armar una posible definición de lo que es la huella digital (se debe hacer énfasis a los alumnos que no existe respuesta correcta e incorrecta, pues sólo es una dinámica de inicio e introducción al tema).

Actividades para iniciar la sesión:

"Dime qué compartes y te diré quién eres."

PARTE 1

El profesor (a) entregará un sobre y un **formato del perfil de Facebook** a cada alumno. En el formato se les pide a los alumnos que peguen las fotos y recortes, asimismo, se deberán llenar los espacios donde se pide información, por ejemplo, nombre, fecha de cumpleaños, lugares que visitaste, estado emocional, etc. También pueden agregar alguna otra información que les gustaría mostrar en su perfil para que las personas conozcan sobre ellos.

El formato con fotos y recortes deberán depositarse en el sobre. Posteriormente, el profesor(a) pedirá que entreguen los sobres y comentará que la información que introdujeron en el sobre ya no se puede quitar y continuará con la siguiente plantilla.

Plantilla 2:

El rastro que dejamos en internet conforma nuestra identidad digital, a través de nuestros comentarios y participaciones en portales, blogs y redes sociales, así como en las búsquedas que realizamos, mostramos nuestros gustos, preferencias u opiniones sobre diversos temas.

Por lo que la identidad digital puede ser definida como las cualidades que nos identifican y definen dentro de internet, es decir, la forma en que somos percibidos por otros usuarios; los datos que conforman nuestra identidad pueden ser:

- formales (se comparten de forma consciente),
- datos informales (datos que proporcionamos de forma inconsciente),
- datos reales (que coinciden con nuestra identidad *offline*) y,
- datos imaginarios (lo que compartimos y que no coincide con nuestra identidad *offline, es decir, el postureo*).

Sugerencias para ejemplificar: datos formales como la fecha de cumpleaños, datos informales como la ubicación o lugar donde nos encontramos, datos reales como imágenes que representan nuestros gustos o intereses y datos imaginarios como fotos de cosas o lugares que aparentamos agradar para ser aceptados o por presunción.

Plantilla 3:

Los datos que conforman nuestra identidad son compartidos a través de:

-Perfiles personales en redes sociales generales y de búsqueda de empleo y portales: son una especie de ficha a través de las cuales se comparten datos generales como nombre, ciudad de residencia, edad, formación académica, fotografía de identificación, etc.

-Comentarios: participaciones que hacemos en foros, blogs, portales de información y redes sociales, estas participaciones pueden ser comentarios, reacciones, publicaciones, repost o retweets.

-Contenidos digitales: Imágenes en redes sociales, videos, presentaciones, documentos, web personal, blogs.

-Contactos: son aquellas personas con las que interactuamos a través de redes sociales, blogs y portales; éstas pueden ser amigos, profesionales que nos siguen o seguimos, empresas, causas; pueden ser personas físicas o morales que conozcamos o no en la vida *offline*.

-Correo electrónico: Son los datos guardados en las bases de datos de las plataformas de mensajería electrónica (direcciones, contacto de correo electrónico y contenido del mensaje con los que interactuamos).

-Mensajería instantánea: existen diversas aplicaciones de mensajería instantánea, entre las que destacan WhatsApp, Messenger y Telegram, en las que interactuamos con los otros por medio de comentarios, estados, fotografías, vídeos, etc. estas interacciones conforman parte de nuestra identidad digital y no son propiamente una red social.

Ejemplo: Nuestras computadoras, dispositivos móviles, tabletas y demás dispositivos con conexión a internet tienen un número que los identifica (llamado IP), todos poseen un número único e irrepetible. Es a través de este número que revelamos información personal cuando enviamos un correo electrónico, por ejemplo, se puede rastrear la ubicación geográfica desde la cual fue enviado el correo.

De igual forma se puede llegar a obtener información sobre el uso y acceso a internet por parte de quien utiliza ese número IP, así como también nombre de usuario, teléfono, fotos compartidas, páginas visitadas, búsquedas en la web y demás información.

Infografía Redes sociales: En este momento de la sesión el profesor (a) entregará una muestra de la infografía por equipo y dará un minuto para que las analice. Tomará al azar 3 papeles (con los nombres de los representantes de los equipos) y a cada uno se le pedirá que responda una de las siguientes preguntas:

1. ¿Por qué crees que el 50% de los usuarios de redes sociales pasan alrededor de 20 horas en ellas?

a. Respuesta esperada o que se debe orientar para llegar a ella: Debido a que no administran de forma inteligente su tiempo.

2. ¿Qué crees que puedes conocer por medio de internet?

a. Respuesta esperada o que se debe orientar para llegar a ella: Internet no tiene límites, puedes conocer desde las noticias del día hasta nuevos idiomas y culturas.

3. ¿Por qué piensas que se te recomienda no mentir en tu perfil de Facebook?

a. Respuesta esperada o que se debe orientar para llegar a ella: Debido a que existen muchos riesgos que pueden comprometer su seguridad, dañar su autoestima, atentar contra alguien más, entre otros. Se requiere que tengan un comportamiento cauteloso y más reflexivo sobre las consecuencias de sus actos.

Plantilla 4:

La huella digital es todo rastro que queda registrado en internet la cual subyace a nuestra identidad digital, es decir, lo qué mostramos, compartimos, visitamos, comentamos y buscamos, pues la mayoría de estos datos quedan almacenados en la red por medio de bases de datos; por lo que, aunque creamos que "borramos" algunos de dichos datos, éstos pueden ser recuperados debido a este registro denominado huella digital.

Ejemplo: cuando subimos una foto a facebook o un video a youtube y lo borramos, en realidad no desaparece. Aparentemente desaparece de nuestro perfil o de nuestra cuenta. Sin embargo, existen bases de datos que almacenan todo y con programas especializados se puede encontrar todo aquello que los usuarios "borraron de internet".

Plantilla 5:

Al hablar de comunicación 2.0 hace referencia a un cambio en la forma de concebir la forma de comunicación entre las personas. De este modo, la comunicación 2.0 se refiere por ejemplo a la aparición de las redes sociales, como Facebook que es una red social mediante la cual los usuarios pueden mantener contacto con amistades e intercambiar contenido como fotos, comentarios y memes a través de internet.

De esta forma el simple hecho de dar "me gusta" a la foto que comparte un amigo en Facebook se considera un tipo de comunicación en el que se envía un mensaje que da a saber que el contenido que subes y compartes en tu red social es de agrado para los demás.

Estos nuevos medios sociales suponen la ruptura del esquema de comunicación tradicional (emisor-receptor, mensaje, canal y código) para convertirla en una

dinámica comunicativa bidireccional y multiformato. Los usuarios de plataformas 2.0 actúan como consumidores y productores de contenidos, por ello, son llamados prosumidores.

Ejemplo: En Facebook los usuarios consumen contenido como ver videos y también producen contenido como compartir un meme.

Infografía Prosumer:

En este momento de la sesión el profesor(a) entregará una muestra de la infografía por equipo y dará un minuto para que las analice. Tomará al azar 3 papeles (con los nombres de los representantes de los equipos) y a cada uno se le pedirá que responda una de las siguientes preguntas:

1.- ¿Por qué crees que dar un "me gusta" te convierte en prosumer?

a. Respuesta esperada o que se debe orientar para llegar a ella:

Porque cualquier interacción que tengamos en la red, provoca un estímulo en la persona que subió el contenido, por lo tanto, es considerada comunicación entre ambas partes, aunque no haya una sola palabra, un "me gusta" ya es un mensaje.

2.- ¿Por qué crees que es importante denunciar un abuso en las redes sociales?

a. Respuesta esperada o que se debe orientar para llegar a ella:

Porque un *prosumer* que hace daño a alguien más, no está capacitado para usar este tipo de redes sociales. Se sugiere que se le denuncie para evitar que siga perjudicando a otros usuarios.

3.- ¿Por qué crees que se sugieren reglas para compartir contenido en la red?

a. Respuesta esperada o que se debe orientar para llegar a ella:

Porque de esta forma cuidamos nuestra huella digital, de igual manera nos aseguramos de no dañar la huella digital de alguien más, así como su integridad, seguridad, autoestima, entre otros. Es decir, debemos pensar dos veces en las consecuencias que puede traer el publicar o compartir cierto contenido, ya sea sobre nosotros o sobre alguien más.

Plantilla 6:

Nuestra huella digital se va conformando al navegar en internet ya que los usuarios dejan un rastro por todos los sitios web, redes sociales y dispositivos (tablet, teléfonos móviles, Pc, etc.) que utilizan, una de las principales formas en que se almacenan nuestros datos son las cookies, éstas se generan cuando

visitamos sitios web e introducimos algunos datos como contraseñas o datos personales, dichos datos son almacenados en nuestros navegadores con la finalidad de ser consultados por el mismo sitio web; a través de las cookies se puede conocer todas las actividades y consultas que hemos realizado a través de la red.

A partir de la aparición y popularización de las redes sociales, todos nuestros comentarios, *tweets*, likes, vídeos, conversaciones, etc. son almacenados en los servidores y bases de datos de dichas aplicaciones web, aunque después estos sean borrados por los usuarios, dejan ciertos rastros con los cuáles se puede conocer las actividades principales que los usuarios realizan en tales redes sociales.

Así mismo sucede con los dispositivos que utilizamos, pues a través de los sitios web y aplicaciones se puede saber cuáles, desde qué dispositivos o direcciones IP realizamos nuestras actividades habitualmente. Esto quiere decir que el Internet sabe que eres la misma persona entrando desde diferentes dispositivos.

Ejemplo: muchas personas descargan música de forma ilegal en internet, es decir, no pagan por obtener una canción o un video, sino que logran hacerlo de forma gratuita. Aunque la persona borre el programa que utilizó en algún momento para descargar la música, el registro de la actividad de descargas queda almacenado y si alguien desea, puede conocerlo.

Plantilla 7:

Pareciera que todos los datos que compartimos a través de internet son sólo compartidos con nuestros contactos, sin embargo, las redes sociales, así como los portales en donde llenamos formularios o subimos fotos y videos, tienen bases de datos almacenadas en servidores físicos o virtuales, es ahí en donde se encuentra toda nuestra información. Es por ello que es de suma importancia conocer los términos de privacidad de cada una de las aplicaciones que descargamos y a través de las cuales compartimos nuestra información, ya que así sabemos qué puede hacer o no la empresa responsable de la aplicación con nuestros datos.

Por otro lado, debido a que a través de la información compartida por medio de redes sociales se pueden conocer datos personales de los usuarios, hace que los perfiles sean blancos de cibercrímenes tales como robo de identidad, ciberacoso, grooming, phishing, ransomware, revelación de identidad, sextorsión o acceso a contenidos inapropiados.

Ejemplo: El Phishing (suplantación de identidad) es un blanco muy común de los perfiles adolescentes debido a que no tienen una adecuada configuración de seguridad, en la mayoría de estos tipos de crímenes se descargan las fotos públicas de los usuarios para crear un perfil en alguna red social con éstas, estos casos son tan comunes que existe un programa de televisión llamado CATFISH (mentiras en la red), en el cual se exponen perfiles creados con fotos de alguien más que han sido utilizados para establecer relaciones amorosas online o a larga distancia, para finalmente descubrir que se ha estado enamorado de la imagen de otra persona. El Ransomware es un tipo de virus que accede a tus datos y archivos y pide una recompensa por devolverte tus datos, uno de los casos más representativos de este crimen se dio a través de un mensaje maliciosos a los usuarios de Skype, en donde aparecía el mensaje "Jaja ¿es esta tu nueva foto de perfil?", al dar clic a tal mensaje comenzaba la descarga de un archivo zip que bloqueaba los datos de los usuarios por 48 horas si no pagaban una recompensa, si se cumplían 48 horas y no se realizaba el pago los datos eran borrados de forma permanente.

Plantilla 8:

Al ser conscientes que muchos de nuestros datos se encuentran almacenados en bases de datos y servidores y que pueden en algún momento ser blanco de cibercrímenes; debemos ser muy cuidadosos con la información que compartimos en formularios y redes sociales, pero debemos hacer énfasis en proteger nuestros datos personales; estos comprenden datos como nuestro nombre, edad, formación académica y número telefónico; puesto que dichos datos en manos de desconocidos pueden ser utilizados para robo de identidad, creación de perfiles falsos u otros crímenes no virtuales como la extorsión o secuestro.

Existen otro tipo de datos que, por sus características, su uso indebido puede afectar gravemente la integridad de la persona, éstos son los denominados: datos personales sensibles. Estos comprenden parte de la ideología de la persona como sus preferencias religiosas, políticas y morales, así como su origen étnico y la información que refiere a su salud y vida sexual, básicamente son todos aquellos datos que puedan ser ocupados por terceros para discriminar, chantajear o extorsionar a la persona titular de los datos.

Ejemplo: un dato personal sensible es la preferencia sexual. Un adolescente puede SER chantajeado por compañeros que amenazan con revelar a sus padres su preferencia por el mismo sexo. Debido a que el chico ha publicado fotos con su pareja en su red social y los compañeros han visto dichas publicaciones.

Plantilla 9:

Tanto los datos personales como los datos personales sensibles deben ser protegidos ya que existen diversos riesgos que pueden comprometer nuestra integridad:

- Modificación: La modificación de datos es básicamente el cambio de algunas configuraciones, contraseñas, comentarios, fotografías, etc. las cuales pueden hacer difícil su recuperación.
- Robo: El robo de datos implica que estos puedan ser utilizados para la suplantación de identidad.
- Divulgación no autorizada: Es el robo de estos con la intención de darlos a conocer sin nuestro permiso ya sea a nuestros conocidos o a personas ajenas a nosotros.
- Extravío y/o eliminación: Refiere a la pérdida o modificación de datos que no puedan ser recuperados por nosotros de acuerdo con los términos de privacidad de los sitios o redes sociales de los que fueron eliminados tales datos.
- Daño a la reputación: Es la divulgación no autorizada de nuestros datos con la intención de afectar y modificar nuestra identidad de forma malintencionada.
- Fraude y Afectación del patrimonio: Refiere a estafas realizadas de forma virtual, a través de una intercepción como un link o la descarga de un archivo, en donde se piden o se hackean los datos personales con la finalidad de realizar alguna transacción financiera sin autorización tales como una compra o la adscripción de un servicio. Afectando directamente la situación financiera del usuario.

Ejemplo: en Facebook existe el apartado de configuración y privacidad, en donde podemos activar o desactivar lo que queremos que nuestros amigos vean en nuestro perfil o lo que no queremos que desconocidos conozcan y vean sobre nosotros.

Plantilla 10:

La Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) plantea las condiciones bajo las cuales los datos personales pueden ser utilizados por terceros.

El INAI es un organismo encargado de la protección de datos personales. Tienen la función de dar a conocer este derecho entre la sociedad mexicana, de promover que se lleve a cabo y vigilar su correcta implementación. El Instituto tiene acceso a bases de datos de las empresas con el fin de supervisar el debido cumplimiento. Si el usuario no está satisfecho con lo que la empresa respondió al ejercer el derecho de acceso, rectificación, cancelación u oposición, o bien, no obtuviste respuesta, puede acudir al INAI. Mediante un procedimiento sencillo y expedito, el Instituto atenderá la solicitud.

Principios:

1) Licitud: Se refiere al compromiso que deben asumir los entes privados (personas físicas o morales) que traten tu información cuando solicitas la prestación de un bien o servicio, respetando en todo momento la confianza que depositas en ellos para el buen uso que les darán a los datos.

2) Consentimiento: Al ser tú el dueño de los datos, este principio te permite decidir de manera informada, libre, inequívoca y específica si quieres compartir tu información con otras personas. Las empresas deben solicitar tu autorización de forma oral y escrita para que pueda tratar la información que te concierne, sobre todo cuando se trata de datos sensibles que afectan tu esfera más íntima.

3) Calidad: Los datos personales en posesión de empresas deben estar actualizados y reflejar información real. Asimismo, implica que el tiempo que esa empresa conserve tus datos no debe exceder un uso más allá de lo necesario. Cuando se cumpla la finalidad para la cual se proporcionaron los datos, el tratamiento deja de ser necesario y las empresas deben cancelarlos.

4) Información: Se refiere al poder que te otorga la Ley de conocer previamente las características del uso que tendrán los datos personales que proporciones a una empresa. En un lenguaje comprensible, las empresas y las personas físicas deben dar a conocer esas características a través del "Aviso de Privacidad".

5) Proporcionalidad: Las empresas sólo podrán recabar los datos estrictamente necesarios e indispensables.

6) Responsabilidad: Quienes traten datos personales deben asegurar que ya sea dentro o fuera de nuestro país, se cumpla con los principios de protección de datos personales, comprometiéndose a velar siempre por el cumplimiento de estos principios y a rendir cuentas en caso de incumplimiento.

El **derecho al olvido** es un derecho relacionado con la protección de datos personales, es decir, es el derecho que tiene el titular de un dato personal a borrar o bloquear información personal.

Esto comenzó en España cuando un hombre pidió que borraran de internet información sobre sus propiedades. El caso terminó en un tribunal europeo que por primera vez exige que se respete el "derecho al olvido" de un usuario en Internet.

Buscadores como Google, son los responsables de procesar y almacenar la información, por lo tanto, deberían también ser los responsables de brindar la seguridad de que los usuarios puedan borrar información personal de internet que les afecte negativamente. Google ya trabaja en el desarrollo de una herramienta que permitirá a los usuarios acogerse al llamado "derecho al olvido" en Internet.

En México, el INAI ha apoyado el derecho al olvido sin considerar los dos elementos a que se refiere la regla C 131/12 de la Comisión Europea, es decir, que el derecho al olvido sólo procede en casos que no tengan relevancia pública ni interés histórico. Y aun así no es infalible, ya que, si alguien contaba de manera personal con esa información, puede maliciosamente volver a subirla.

Ejemplo: los bancos son instituciones que poseen gran cantidad de datos personales y confidenciales. El INAI protege que se utilicen de forma correcta dichos datos, o actuar en caso de que se haga un mal uso con ellos.

Infografía Identidad digital: En este momento de la sesión el profesor (a) entregará y pedirá a todos los equipos que lean la infografía de Identidad digital (contarán con 5 minutos para ello), posteriormente al azar tomará 3 papeles (con los nombres de los representantes de los equipos) y a cada uno se le pedirá que responda una de las siguientes preguntas:

1.- ¿De qué forma proteges tu identidad digital?

a. Respuesta esperada o que se debe orientar para llegar a ella: cuidando toda la información que pongo y comparto en internet sobre mí, por ejemplo, en instagram, pensar cuando comparto el lugar donde estoy, fotos que subo o comentarios que hago.

2.-Menciona algunos riesgos a los que está expuesta tu identidad digital

a. Respuesta esperada o que se debe orientar para llegar a ella: riesgo a que roben mi identidad, robo de mis datos personales, información falsa sobre mí, y otros riesgos como bullying o que roben fotografías mías.

3.- ¿Por qué crees que es importante cuidar tus datos personales?

a. Respuesta esperada o que se debe orientar para llegar a ella: porque son datos confidenciales y si estos llegan a estar en manos de personas desconocidas, corren el riesgo de hacer con ellos un uso inadecuado.

Plantilla 11:

Visibilidad: Hoy en día la vida virtual es tan o más importante que la real. Todos quieren salir espléndidos en las fotos que suben y mostrarse como personas sociables-populares.

Los *"me gusta"* en Facebook, las visitas en YouTube y los seguidores en Twitter se pueden comprar. Es decir, existen usuarios que no tienen gran cantidad de seguidores o *likes*, por ello, en México la empresa *Shopatia Technologies* se dedica a crear *bots*: robots de internet que sirven para aumentar automáticamente la cantidad de tuits, *likes* en fotos o visitas en youtube.

Quien adquiere los *bots* puede elegir su sexo, edad, lugar de origen de quienes lo seguirán e incluso programarlo para que el aumento en visitas o amigos no se note y se dé gradualmente.

Se pueden obtener 50 mil seguidores en *Twitter* por 3,900.00 pesos. Para Facebook, se pueden obtener 900 fans por 400 pesos y cada "*Me gusta*" vale 44 centavos. En YouTube es posible comprar 2.500 visitas por 400 pesos.

Las frases y el contenido de las respuestas que son publicadas son controladas por el usuario, mismo que puede programar las frases y los tiempos para las publicaciones del contenido que desea publicar. Así que para querer y parecer popular se necesita dinero y un mínimo de creatividad.

Aunque parezca una buena idea comprar seguidores, *likes* o visitas en YouTube para ser "popular", sin embargo, el realizar esta acción tiene algunas consecuencias negativas, por ejemplo:

-No se tiene una interacción real con los seguidores porque en realidad estos son robots que no son conscientes de lo que dicen en tus publicaciones.

-Pierdes credibilidad en caso de que tus seguidores o la página social detecte que estás consiguiendo seguidores de forma fraudulenta, por ende, el crear nuevamente una imagen positiva será más difícil.

-Mejor es la calidad y no la cantidad, puesto que de nada nos sirve tener miles de seguidores que estén en silencio, que no les interese el contenido que se publique o que sean incoherentes en sus comentarios.

-No hay garantía de permanencia, ya que nada te garantiza que los seguidores falsos, que hayas comprado, te seguirán por siempre. Es mejor tener pocos seguidores pero que estos sean reales y realmente sigan el contenido que publicas.

-Puede llegar afectar la autoestima, pues imaginariamente construimos la idea de que tenemos muchos amigos y somos muy populares, pero en realidad son personalidades falsas que no les interesa en lo mínimo el contenido que publicamos y que no saben ni quienes somos.

Privacidad: Controlar nuestra privacidad es importante. Utilizamos muchas aplicaciones y redes sociales que tienen acceso a una gran cantidad de información sobre nosotros. Entre ellas, Facebook es posiblemente una de las que más nos conoce. Más allá de la propia empresa, es vital también configurarla correctamente para que desconocidos no puedan saber quiénes somos o para que nuestros amigos solo vean aquello que nos interesa.

Cualquiera puede encontrar nuestro perfil de Facebook con sólo insertar nuestro nombre. Si no queremos que esto sea así, se puede limitar el acceso a determinada información personal. Por ejemplo, en Facebook existe un apartado de ajustes de privacidad en donde se especifica y delimita qué información y contenido es el que queremos que sea visible para nuestros amigos. Algunas cosas que puedes controlar son las siguientes:

Elegir quién ve mis fotos, eliminar una foto o contenido que no deseaba haber publicado, comprobar lo que otros ven en mi perfil, controlar que otros vean o no mi lista de amigos, quién puede ver mis comentarios, quién puede enviar solicitud

de amistad, elegir amigos de confianza para que me ayuden en caso de que pierda el acceso a la cuenta.

Reputación: El gran aumento de las redes sociales ha provocado gran curiosidad por saber la vida de las personas y las actividades que realizan a diario. En algunos casos una mala reputación de Facebook tiene consecuencias muy reales, por ejemplo, la pérdida de una buena oferta de trabajo. A continuación, se presentan algunos consejos sobre cómo tener una reputación positiva que tenga buenos efectos en nuestras relaciones interpersonales tales como; pensar antes de publicar algún contenido que afecte mi persona o a otros, controlar la privacidad de lo que publico y ser uno mismo (no tratar de aparentar algo que no somos).

Ejemplo: visibilidad (aparentar que visito lugares lujosos como restaurantes) privacidad (revisar que mis datos personales como teléfono y dirección no sean visibles en mi perfil de Facebook) y reputación (cuidar de no subir fotos que afecten negativamente mi persona o evitar hacer comentarios desagradables de otros).

Plantilla 12:

Asegurarnos que las páginas a las que ingresó cuenten con filtros de seguridad que protejan los datos personales: Al ingresar a páginas web es importante identificar el apartado donde se especifica el uso y privacidad que se les dará a nuestros datos personales, en la mayoría de las páginas aparecen al final del sitio.

Verificar el uso que le dan a mis datos que recolectan determinadas páginas: cuando ingresamos a páginas web o al descargar alguna aplicación, el sistema arroja avisos de privacidad, que también son conocidos como términos y condiciones de privacidad (esto se refiere a la confidencialidad o uso que le darán los datos personales que insertamos en la aplicación o en la página) . En algunos otros casos las páginas cuentan con condiciones de uso, es decir, establecen normas que dicen cómo y cuál es el uso que le puedes dar al contenido de dicha página.

Evitar hacer compras o transferencias bancarias en lugares públicos: hacer compras o transferencias bancarias implica ingresar datos confidenciales como números de cuenta y contraseñas. Por ello, no es recomendable hacerlo en computadoras del uso público o en wifi públicas.

Cambiar con frecuencia mis contraseñas: una contraseña con alta seguridad es aquella que está compuesta por números, letras mayúsculas y minúsculas. A continuación, se hacen una serie de recomendaciones que mantendrán a salvo nuestros datos personales y confidenciales tales como; no compartir nuestras contraseñas (ni con personas consideradas de confianza), no utilizar la misma contraseña para diferentes cuentas, cambiar las contraseñas frecuentemente y no utilizar fechas de cumpleaños o datos obvios y sencillos de adivinar por desconocidos.

Ejemplo: Cuando descargamos y utilizamos Netflix es importante conocer el uso que le darán a nuestros datos de tarjeta con la que se hace el cobro por utilizar la aplicación. Estos términos se encuentran en el apartado de cuenta, en el rubro de declaración de privacidad y términos de uso. Comúnmente los usuarios que cuentan con una suscripción a Netflix suelen compartirla con varias personas, ya sean amigos, familia y/o conocidos. Esto también pone en riesgo nuestros datos personales, ya que al darles la oportunidad de entrar a nuestro usuario también les estamos dando la oportunidad de entrar a nuestra información personal y confidencial. Por lo que se recomienda no compartir este tipo de cuentas.

Una nueva forma de crear contraseñas seguras es a través de passphrases en vez de passwords, es decir, contraseñas conformadas por acrónimos de frases, por ejemplo: tengo 2 perros salchichas llamados Bongo y Max: t2pslIByM.

Plantilla 13:

Navegar en internet, entrar a sitios de entretenimiento, realizar búsquedas de lo que sea o incluso introducir datos personales no es malo, actualmente muchos sitios requieren que se proporcionen ciertos datos incluso para identificar el uso correcto de los recursos que ofrece un sitio web, página o aplicación. Lo importante es ser consciente de lo que estamos aprendiendo de internet, saber que no todo lo que aparece en línea es bueno y que todo lo que hagamos en la red jamás desaparecerá, lo cual afectará de forma positiva o negativa en nuestras relaciones sociales, laborales, profesionales. Por lo que se vuelve muy importante ser consciente del objetivo o motivo por el cual hacemos uso de las pantallas.

Ejemplo: podemos utilizar con mucha frecuencia Facebook, pero lo importante es utilizar con fines positivos compartiendo contenido, fotos e información constructiva.

Actividades para concluir la sesión:

"Dime qué compartes y te diré quién eres."

PARTE 2

El profesor sacará los sobres que trabajaron al inicio de la sesión, irá uno a uno sacando los sobres planteando para cada uno alguna de las siguientes situaciones:

-Este sobre se entregará a su futuro jefe, cuando ingresen al trabajo de sus sueños.

-Este sobre se entregará a su mamá en su lecho de muerte.

-Este sobre se entregará a su futuro esposo(a) el día de su boda.

-Este sobre se lo voy a entregar a la primera persona que me encuentre en el metro.

-Este sobre lo entregaré a su primer hijo cuando cumpla 15 años.

-Este sobre se lo voy a entregar a su crush su último día en secundaría.

-Este sobre lo voy a pegar en la entrada de la escuela.

-Este sobre se lo voy a entregar a la señora de la tiendita de mi casa.

-Este sobre se lo voy a entregar a tus maestros de la Universidad.

-Este sobre se lo voy a entregar a tu futura suegra.

- No es necesario mencionar todas las anteriores, queda a criterio del profesor.

Para finalizar la actividad el docente explicará que la dinámica realizada fue una simulación del uso que se le da a las redes sociales en la vida real y se les regresa el sobre con su información personal.

Después harán las siguientes preguntas:

-¿Qué sientes al pensar que una persona desconocida tiene tu información personal sin que directamente se la des?

-¿Qué piensas acerca de que tus datos, tus contraseñas, tus búsquedas y descargas de contenido o las visitas que haces a sitios web queden guardados en algún lugar del ciberespacio y nunca se puedan borrar por completo?

-¿Cómo protegerías tus datos e información personal?

Se toman de 3 a 7 participaciones de los alumnos.

Veamos un vídeo:

Se presenta el **video** sobre huella digital.

Al terminar el vídeo el docente les pide a los alumnos que respondan para sí mismos ¿Ustedes para qué ocupan internet?, ¿Transforman su mundo con sus acciones en internet? y ¿Cómo podrían hacer de un mundo mejor para todos a través del uso de internet?

Encuentra información adicional en:

Barragán, V. & Terceros I. (2017). *Radios, redes e internet para la transformación social.* Ecuador: CIESPAL.

Dans, I. (2015). Identidad digital de los adolescentes: la narrativa del yo. *Revista de Estudios e Investigación en Psicología y Educación, 0*(13), 001-004. doi:http://dx.doi.org/10.17979/reipe.2015.0.13.145

Fundación Telefónica. (2013). *Identidad Digital: El nuevo usuario en el mundo digital.* España: Fundación Telefónica. Recuperado de: http://boletines.prisadigital.com/identidad_digital.pdf

Familia digital : http://familiadigital.net/resources

Ochoa, Gutierrez, P. y Uribe, Alvarado, J. (2015). Sentido de la interacción social mediada por facebook. En estudios sobre las culturas contemporáneas, XXI (42), 9-37. Colima.

Homayoun, A. (2017, junio, 14). La vida secreta de los adolescentes en facebook (blog). Recuperado de https://www.google.com/amp/s/www.nytimes.com/es/2017/06/14/redes-adolescentes-precauciones/amp/