Enero 2016

CAMPOS FORMATIVOS:

Programa Civismo Digital - Escolar
Material Educativo

Lección: **TU IDENTIDAD EN INTERNET** v. 1.0
Topico: **Alfabetización Digital, Huella Digital**

Objetivo:
Fomentar en los alumnos la importancia de cuidar su identidad digital, entendiendo que constituye la representación de ellos mismos en el mundo virtual, destacando la relevancia de utilizar siempre contraseñas seguras.

Materiales:
- Copia de la ficha "Manejo de contraseñas sólidas" por cada alumno
- Pizarrón

Vocabulario:
Nickname
Nombre que identifica una cuenta para un servicio o recurso en Internet
Contraseña
Clave secreta que permite tener acceso a un servicio.

Para Familias:
Ficha "Cuidado de la Identidad en Internet"

Preparación:

Pregunta:	**¿Qué es una llave?**
Reflexión:	**Una cerradura sólo se puede abrir con la llave adecuada, pero que si le damos una copia a otra persona, podría abrirla igual que con la original.**

La identidad digital se refiere a los elementos que, como su nombre lo indica, identifican al usuario en los diversos servicios de Internet, de redes locales, e incluso, de dispositivos digitales como teléfonos y video consolas, y puede ser diferente para cada uno de ellos.

Los elementos que usualmente componen la identidad digital son:

a) El nombre de usuario (en inglés username o nickname)
b) La contraseña (en inglés password)

ACTIVIDAD 1 Creación de un nombre de usuario (Nickname)

Un usuario puede utilizar una identidad para acceder a su servicio de banca electrónica, y otra diferente para su perfil en redes sociales por ejemplo. Esto es recomendable, ya que en caso de que la identidad digital caiga en manos de un tercero mal intencionado, no podrá ingresar con la misma a todos nuestros servicios. Algunos dispositivos como los teléfonos celulares sólo requieren de una clave o contraseña para bloquear o desbloquear el dispositivo, pero no solicitan un nombre de usuario.

En servicios de Internet, como portales de comercio electrónico, reservaciones de viajes, redes sociales, etc…, es común que el nombre de usuario sea la propia dirección de correo electrónico del usuario.

Para el caso de servicios que solicitan un nombre de usuario que no sea la dirección de correo electrónico, se recomienda utilizar nombres neutrales, que no tengan nada que ver con la persona, para que no puedan ser adivinados por individuos mal intencionados, que después traten de descubrir también la contraseña del titular y acceder a los servicios sin autorización, y cometer fraudes, suplantación, y otra serie de calamidades.

Por ejemplo, si el usuario es reconocidamente aficionado al futbol, no sería buena idea que su nombre de usuario fuera algo como “Soccermaster”, o “Supersoccer”, a algo así, porque al igual que la contraseña, puede ser adivinado con mayor facilidad.

En el caso de los niños, es recomendable orientarlos para que no incluyan su edad como parte de su nombre de usuario, ni su género, es decir, si son niñas o niños. Los siguientes **no son nombres de usuario recomendables**:

susyglz_12	¡evitar!
carlitos_11	¡evitar!

Las contraseñas se han convertido en una parte fundamental de la identidad digital de todos los usuarios de internet, pues protegen el acceso a sus diferentes cuentas, información y servicios.

Los usuarios de internet en general han experimentado una gran cantidad de problemas por utilizar contraseñas débiles o fáciles de adivinar, lo que los ha convertido en ocasiones en víctimas de accesos no autorizados a su información y servicios, por lo que resulta de gran importancia conocer la mecánica para construir contraseñas más seguras.

ACTIVIDAD 2 Manejo de contraseñas seguras.

El lugar donde Ud. vive tiene puertas y ventanas, y quizá la mayor parte del tiempo ellas estén cerradas. Para cada cerradura que utiliza hay una llave, las probabilidades indican que cada llave es diferente. Usted sabe que debe cerrar y no compartir las llaves con extraños, y probablemente no con la mayor parte de sus amigos. Usted no debe esconder sus llaves bajo la estera ni en una maceta en su jardín.

Las contraseñas para computadoras son casi lo mismo. Para cada computadora y servicio que utiliza (comprar en línea, por ejemplo), usted debe tener una contraseña. Cada contraseña debe ser única y no relacionada a cualquiera de sus otras contraseñas. Usted no debe mantenerlas escritas en ningún lado, ni las debe compartir con nadie, aún sus mejores amigos.

Eche una mirada a su llave de la puerta principal. Es bastante complicada. Hay muchos cortes y ranuras. Si no hubiese tantas variaciones posibles, un ladrón podría hacer fácilmente una llave para cada combinación posible y entonces tratar cada una en su puerta principal. Este método del ensayo y el error, (llamado **fuerza bruta** en computación) tienen probabilidades de ser efectivo incluso si toma mucho tiempo a un intruso. Sin embargo, por mucho que sea complicado, si el ladrón obtiene su llave, él o ella la pueden copiar y usarla para abrir su puerta.

Una contraseña también puede ser compleja. La mayoría de los esquemas permiten que usted utilice cualquier combinación de letras (mayúsculas o minúsculas), números, y algunos permiten también que usted utilice los signos de puntuación. Las longitudes pueden variar. Usted puede crear una contraseña para ser tan compleja como usted quiera. La clave consiste en que Ud. deberá ser capaz de recordar esta contraseña siempre que la necesite sin tener que escribirla para ayudar a su memoria.

Como el ladrón en su puerta, intrusos de computadora también utilizan el método del ensayo y error, o las técnicas de la fuerza bruta para descubrir las contraseñas. Bombardeando un punto de la entrada (login) con todas las palabras en un diccionario, ellos pueden “descubrir” la contraseña que permita el acceso. Si ellos saben algo acerca de usted, tal como el nombre de su esposo/a, la clase de coche que usted maneja, o sus intereses, intrusos listos pueden reducir la gama de contraseñas posibles y tratar esas primero. Ellos son a menudo exitosos. Las variaciones aún leves, tal como agregar un dígito en el fin de una palabra o reemplazar la letra O con el dígito 0 (cero), no son suficientes para proteger sus contraseñas. Los intrusos saben que utilizamos estas artimañas buscando que nuestras contraseñas sean más difíciles de adivinar.

Como la llave de una puerta principal, aún una compleja contraseña se puede copiar y la copia utilizarse exactamente igual que la original. Si un día encuentra la puerta de su casa abierta, muy difícilmente podría saber si se abrió utilizando la llave original, o una copia.

Lo mismo sucede con una contraseña. Si usted se la dice a otra persona, aún de su confianza, sería muy difícil determinar en un momento dado quien la utilizó para acceder a un equipo, sitio o servicio.

¿Recuerda la discusión previa acerca de cómo información en el Internet puede ser vista? Suponga que la contraseña realmente fuerte que a usted le tomó mucho tiempo crear – una larga con 14 caracteres, incluyendo 6 letras, 4 números y 4 signos de puntuación, todo en orden aleatorio – viaja a través del Internet libremente. Un intruso puede ser capaz de verla, guardarla, y utilizarla después. Esto se llama 'Olfatear' (sniffing) y es una práctica común de un intruso. Por esta razón, es muy importante verificar que cualquier sitio que solicite nuestras contraseñas, sea un sitio seguro.

El punto es que usted necesita seguir la práctica de utilizar una contraseña única con cada cuenta que tenga. Más adelante encontrara un conjunto de pasos que puede utilizar para ayudarse a crear las contraseñas para sus cuentas:

1. La prueba de **Solidez**:
   ¿La contraseña es suficientemente sólida (esto significa la longitud y el contenido) como las reglas de la cuenta lo permita?

2. La prueba **Única**:
   ¿La contraseña es única y no relacionada con cualquiera de sus otras contraseñas?

3. La prueba **Práctica**:
   ¿Usted puede recordarla sin tener que escribirla?

4. La prueba **Reciente**:
   ¿Usted la ha cambiado recientemente?

A pesar de las pruebas de **SUPR**, usted necesita estar enterado que ese 'Olfateo' sucede, e incluso la mejor de las contraseñas puede ser capturada y utilizada por un intruso.

Usted debe utilizar las contraseñas no sólo en su computadora doméstica, también para los servicios que usted utiliza en cualquier otra parte en el Internet. Todo debe tener las contraseñas más solidas que usted pueda definir y pueda recordar, y cada contraseña debe ser única y no relacionada a ninguna otra de sus contraseñas. Una contraseña sólida debe ser larga, utiliza las combinaciones de letras en mayúscula y minúsculas, números, y signos de puntuación, y generalmente no son una palabra que se pueda encontrar en un

diccionario. Recuerde también que por fuerte que una contraseña sea, se puede capturar u olfatear si se envía sin encriptar en cualquier lugar en el Internet.

TIP: Utilice iniciales de frases que le sean fáciles de recordar, por ejemplo:

La frase: "**E**l **c**ampeón **d**el **m**undial 2004 **f**ue **B**rasil"

Genera la contraseña: **ecdm2004fb**

Si a esto lo combina con mayúsculas/minúsculas y signos de puntuación, su contraseña será bastante sólida, por ejemplo

ecdM2004fB

Manejo de Contraseñas Sólidas (Passwords)

Por cada cuenta que tenga, llene una línea de la siguiente tabla
(Importante: NUNCA escriba sus contraseñas, ni aquí ni en ninguna parte)

Cuenta	**¿Sólida?** Aprovecha todas las reglas disponibles.	**¿Única?** No se repite en otra cuenta.	**¿Práctica?** Es fácil de recordar	**¿Reciente?** Fecha en que se cambió.

