SECUENCIA DIDÁCTICA

Autenticación con contraseñas

¿Qué hace que una contraseña sea segura? ¿Qué características tienen las claves inseguras? ¿Por qué no deben usarse?

En esta secuencia didáctica se estudian distintos factores que deben tenerse en cuenta para generar contraseñas que sean lo más seguras posible.

Actividad 1. ¿Cuán segura es tu clave?

Partiendo de una situación hipotética para ayudar a un anciano a generar una clave para un cajero automático, se sensibiliza a las y los estudiantes sobre hábitos de seguridad informática para elegir una contraseña.

Actividad 2. La fábrica de contraseñas seguras

Se brindan herramientas para comprender algunos aspectos computacionales que contribuyen a que una contraseña sea segura y se presentan buenas prácticas para generarlas.

Datos curriculares

Nivel: Primario, segundo ciclo

Área: Ciudadanía y Computación

Eje: Estrategias para un uso seguro de internet

Contenido

- Estrategias para la protección de la información privada y la Identidad digital: claves seguras, permisos y sitios seguros.

Objetivos de aprendizaje

- Reconocer claves seguras y no seguras.
- Crear claves seguras fáciles de recordar.

Materiales necesarios

- Fichas para estudiantes.

Todos los recursos necesarios para esta secuencia están disponibles en: https://curriculum.program.ar/
Podés buscarlos por el título de la secuencia.

Acerca de esta iniciativa

Desde el sitio curriculum.program.ar tenemos por objetivo acompañar a la comunidad docente de habla hispana en el desafío de llevar las Ciencias de la Computación al aula.

Para ello, construimos un repositorio que reúne diversos recursos para el aula que desde la Iniciativa Program.AR de la Fundación Sadosky impulsamos desde 2013.

Organizados a partir de los saberes a promover con nuestras y nuestros estudiantes y los conceptos de la disciplina presentados en la Propuesta curricular para la inclusión de las Ciencias de la Computación (CC) en el aula, encontrarán en curriculum.program.ar proyectos, secuencias didácticas y actividades desarrollados por una diversidad de autores y docentes en conjunto con instituciones y universidades de América Latina.

Estos materiales, que han sido desarrollados para responder a necesidades de diferentes contextos y países y que son heterogéneos en su formato y extensión, comparten un mismo propósito: integrar las Ciencias de la Computación en la escolaridad obligatoria para promover en el conjunto de los y las estudiantes la construcción de saberes que les permitan comprender, apropiarse y transformar la tecnología digital y computacional y así participar de manera crítica del mundo contemporáneo.

Cómo utilizar este recurso

Siguiendo la Propuesta curricular, es posible organizar una planificación escolar para el grado o el año a abordar y, a partir de ella, seleccionar del universo de recursos para el aula que ofrecemos los que sean adecuados al contexto y la realidad de cada grupo de estudiantes.

Al acceder a esta secuencia en el sitio curriculum.program.ar, encontrará los enlaces para descargar los materiales anexos que fueren necesarios.

Instituciones

Ministerio de Ciencia, Tecnología e Innovación Argentina

CAF

FAMAF Facultad de Matemática, Astronomía, Física y Computación

UNC Universidad Nacional de Córdoba

Fuente

Areces, C., Benotti, L., Cortez, J. J., et.al (2018). *Ciencias de la computación para el aula: 2do. ciclo de primaria: libro para docentes.* Ciudad Autónoma de Buenos Aires: Fundación Sadosky.
http://program.ar/manual-segundo-ciclo-primaria/

Fundación SADOSKY

<Program.AR/>

Fuente: Imagen de coolvector en Freepik.

Secuencia Didáctica 2

AUTENTICACIÓN CON CONTRASEÑAS

En el famoso cuento “Alí Babá y los cuarenta ladrones”, los malhechores usaban la frase secreta “ábrete sésamo” para abrir las puertas de la cueva donde guardaban los tesoros robados. A lo largo de la historia, distintos tipos de toques, apretones de mano y saludos secretos se han usado como contraseñas entre grupos de personas.

Hoy en día, prácticamente todos necesitamos contar con alguna suerte de palabra secreta o clave para acceder a otro tipo de tesoro: la información valiosa. Ya se trate de redes sociales, juegos o plataformas de compras en línea, lo cierto es que la mayoría de los servicios suele requerir un nombre de usuario y una contraseña.

Existen distintas formas de autenticación de una contraseña, pero el uso de las alfanuméricas es el mecanismo más difundido. En esta secuencia didáctica vamos a estudiar distintos factores que deben tenerse en cuenta para generar contraseñas lo más seguras posibles.

OBJETIVOS

- Identificar cuáles son las características de las claves seguras.
- Crear claves seguras utilizando las características aprendidas.

Actividad 1
¿Cuán segura es tu clave?

DE A DOS

OBJETIVOS

- Sensibilizar a los estudiantes a partir de un juego sobre hábitos de seguridad informática para elegir una contraseña.
- Reconocer algunas acciones de seguridad en el uso de contraseñas.

MATERIALES

Ficha para estudiantes

DESARROLLO

Arrancamos la actividad diciendo a la clase: "Levanten la mano quienes usan contraseñas, por ejemplo, en redes sociales, juegos o para bloquear dispositivos como el celular". Es probable que la mayoría lo haga. Si hay estudiantes que nunca crearon una contraseña, les pedimos que piensen una. Luego, les indicamos que levanten la mano si tienen algunos de los siguientes hábitos relacionados con la seguridad de las claves:

1. Usás tu apodo como clave.
2. Tu clave incluye texto, números y símbolos.
3. Tu clave tiene menos de 8 caracteres (letras, dígitos y otros símbolos).
4. Dejás que tus amigos sepan tu clave.
5. Solo vos y tus padres o tutores conocen tu clave.
6. Tu clave es una palabra que aparece en el diccionario.
7. Te resulta difícil recordar tu clave.
8. Tu clave es un número telefónico.

Algunos puntos corresponden a prácticas seguras (2 y 5) y otros no (1, 3, 4, 6, 7 y 8). Preguntamos: "¿Qué diferencia una contraseña segura de otra que no lo es? ¿Qué tipo de contraseña imaginan que pueden ser más segura?". Es posible que respondan que las contraseñas que tienen al menos 8 caracteres y combinan números, letras en mayúscula y minúscula y otros símbolos son más seguras. Esto es así porque los programas de computación pueden combinar caracteres y hacer muchos intentos para adivinar una clave en segundos. Mientras más larga y compleja sea la clave, más difícil será para una máquina atacante adivinarla.

A continuación, les contamos el caso del abuelo don Braulio, quien ha recibido una tarjeta de débito electrónica por primera vez en su vida. Necesita usar la tarjeta, pero antes debe crear una contraseña. ¿Cómo lo podemos ayudar? Repartimos la ficha para estudiantes y les pedimos que la completen trabajando de a dos.

En la segunda consigna de la ficha, se sugiere que el usuario aplique una serie de reglas para crear una contraseña. La más adecuada de las opciones es la (ii) ya que cumple con todas las reglas: tiene dos mayúsculas, más letras que dígitos y tres símbolos (#@BelBob3r-2688).

CIERRE

Esta actividad revela que muchos de los usuarios, incluyendo adultos, tienen pocos saberes sobre cómo generar contraseñas seguras. Elegir como claves palabras que son fácilmente reproducibles o fáciles de adivinar no es un buen hábito de seguridad informática. Para concluir, sugerimos reflexionar sobre la diferencia de hábitos para crear contraseñas y analizar con toda la clase la temática de la seguridad en claves remarcando qué hábitos son seguros y cuáles no.

NOMBRE Y APELLIDO:

CURSO: FECHA:

¿CUÁN SEGURA ES TU CLAVE?

El abuelo Braulio Martínez nació el 29/02/1950 y su DNI es 10.474.391. Recibió por correo una tarjeta para hacer los trámites del banco desde su casa, pero debe crear una contraseña y no entiende mucho de eso. ¡Ayudalo a elaborarla!

1. Don Braulio probó crear las siguientes contraseñas, pero el sistema le dijo que no eran seguras:

Braulio	braulio290250	braulio1234	elprincipito
Braulio1950	1234	bmartinez	sodaestereo
10.474.391	juanaazurduy	Br@ul10	oidmortales

- ¿Por qué creen que son consideradas inseguras?

2. El banco le solicitó al abuelo que creara la contraseña aplicando estas reglas:

- La contraseña debe contener al menos dos letras mayúsculas.
- La contraseña debe tener más letras que dígitos.
- La contraseña debe contener al menos tres símbolos (que no sean letras ni números).

Mirá con tus compañeros las contraseñas propuestas e indicá cuál es la más adecuada.

☐ HloD@mb2953?

☐ #@BelBob3r-2688

☐ R5#X&v73r68?!

☐ *h9n3ytR33*

☐ BrauLio1966

- ¿Qué otras posibilidades de contraseña se te ocurren? Da 3 ejemplos.

Actividad 2
La fábrica de contraseñas seguras

DE A DOS

OBJETIVOS

- Reconocer claves seguras y no seguras.
- Crear claves seguras fáciles de recordar.

MATERIALES

Ficha para estudiantes

DESARROLLO

Iniciamos la actividad, preguntando: "Cuando ingresan a un sitio en línea que requiere una contraseña, ¿qué tipo de contraseña pueden pedirles para que esta sea segura?". Pueden responden que algunos sitios solo aceptan como contraseña aquellas que tienen al menos 8 caracteres y combinan números, letras en mayúscula y minúscula y otros símbolos.

Retomamos lo visto en la actividad anterior, en la que señalamos que los programas de computación pueden combinar caracteres y hacer muchos intentos para adivinar una clave en segundos. Mientras más larga y compleja sea la clave, más difícil será para una máquina atacante adivinarla.

Si la clave fuera de 3 caracteres y se usaran solo números, sería bastante fácil adivinarla. Bastaría con intentar mil veces. ¿Por qué? Porque desde el 000 al 999 hay 1000 claves posibles. Se sugiere ejemplificar esta situación usando claves de 1 y 2, dígitos ya que la operación que surge es la potenciación. Y para los casos de 1 y 2 dígitos es más simple observar que pasa de 10 a 10x10=100 claves posibles respectivamente.

A través de más ejemplos se puede notar que:

- Para claves de 4 dígitos hay 10^4 = 10.000 posibles claves.
- Para claves de 5 dígitos hay 10^5 = 100.000 posibles claves, y así sucesivamente.

Esto muestra que, aumentando el número de caracteres de la clave, crece exponencialmente la cantidad de intentos necesarios para adivinarla. La insistencia en el uso de símbolos, números y letras es principalmente para que la contraseña elegida sea más difícil de adivinar. Una clave que, además de números, incluya letras y símbolos aumentará mucho la cantidad de combinaciones que va a tener que probar el programa de quien esté tratando de descubrirla.

Usando letras en mayúscula, minúscula, dígitos y 5 símbolos en claves de 8 caracteres, la cantidad de claves posibles se eleva a $(27 + 27 + 10 + 5)^8$ = 513.798.374.428.641 (más de 500 billones). Usando solo letras en minúscula da $(27)^8$ = 282.429.536.4816 (algo más de 280.000 millones) claves y usando solamente dígitos, $(10)^8$=100.000.000 (100 millones). Muchas personas usan nombres, fechas, siglas u otro tipo de palabras como clave porque son más fáciles de recordar. Es importante que una clave sea fácil de recordar para evitar anotarla y que alguien la vea. Pero también es importante pensar en una contraseña que sea difícil de adivinar.

Teniendo en cuenta cómo las computadoras procesan la información para armar combinaciones y así descubrir una clave, entregamos la ficha a los estudiantes y les pedimos que formen parejas y la completen. En la ficha proponemos seguir los pasos de una receta para fabricar contraseñas seguras.

TAREA PARA EL HOGAR

Al final de la ficha, proponemos un juego optativo para que los estudiantes realicen en sus hogares: el ahorcado. La idea es que las primeras tres palabras se jueguen de forma clásica y luego se incorpore una variante. Esta cuarta palabra a adivinar se tratará de una palabra a la que se le aplicarán las mismas reglas que se utilizaron en la fábrica de contraseñas seguras.

¿Qué buscamos con esta variante? Que el otro participante del ahorcado no logre descifrar la palabra. Entonces, después de varios intentos fallidos, se le explicará que a la palabra se le aplicaron una serie de reglas que la vuelven más difícil de adivinar.

CIERRE

Para cerrar lo visto sobre seguridad de contraseñas, recomendamos las siguientes prácticas:

- No usar solamente letras o números.
- No usar palabras reconocibles, tales como nombres propios, palabras del diccionario o términos de televisión, canciones o similares, aun si terminan con números.
- No usar palabras en idiomas extranjeros populares.
- No usar información personal como fechas, números de DNI o de teléfono.
- No escribir contraseñas en papel como recordatorio.

NOMBRE Y APELLIDO:

CURSO: FECHA:

LA FÁBRICA DE CONTRASEÑAS SEGURAS

Te presentamos una receta para fabricar contraseñas seguras. ¡Creá contraseñas que sean fáciles de recordar, pero difíciles de adivinar! Los pasos a seguir son:

1. Pensá una frase cualquiera, por ejemplo: "Somos lo que hacemos para cambiar lo que somos".
2. Anotá cada una de las iniciales de las palabras, una al lado de la otra. Siguiendo nuestro ejemplo, quedaría así: slqhpclqs.
3. Sustituí letras por números. Por ejemplo, la letra h por el número 4 y la q por el símbolo @. Ahora nuestra frase quedaría así: sl@4pcl@s.
4. Colocá en mayúscula al menos una letra, como, por ejemplo, la P. Esto nos da: sl@4Pcl@s

¡ATENCIÓN!
No escribas ni imprimas tus contraseñas en un papel.

1. Aplicá la receta (eligiendo dos o más sustituciones) a las siguientes frases:

"Susanita tiene un ratón, un ratón chiquitín, que come chocolate y turrón". _____

"Oíd, mortales, el grito sagrado: libertad, libertad, libertad". _____

"Cuando bailo un bailecito mi pañuelo es una pluma, va volando entre las nubes acariciando la luna". _____

2. ¿Cuáles son buenas prácticas del uso y la creación de contraseñas?
Leé las oraciones y escribí SÍ o NO según corresponda en cada caso:

Cambiar tu contraseña si sospechás que alguien más entró en tu cuenta. ☐

Usar una palabra del diccionario como contraseña. ☐

Decir a tus padres tu contraseña. ☐

Si creés que alguna de tus contraseñas no es segura, cambiarla pronto. ☐

3. ¿Qué tenemos que hacer cuando vemos que alguien va a escribir su contraseña en una compu o un celular?

☐ Mirar hacia otro lado.

☐ Anotar la contraseña en un cuaderno o celular.

☐ Decirle tu propia contraseña para mostrar que son buenos amigos.

☐ Mirar de cerca y avisarle que no está ocultando la contraseña.

NOMBRE Y APELLIDO:

CURSO: FECHA:

TAREA PARA EL HOGAR: ¡A JUGAR AL AHORCADO![1]

Pedile a algún familiar que juegue con vos al ahorcado. En las primeras tres veces, buscá que adivine las palabras que aparecen en la primera columna de la tabla. A medida que va adivinando, completá las otras columnas de la tabla. ¡Atención! Tu familiar no debe ver las palabras hasta el final del juego.

PALABRA A ADIVINAR	¿ADIVINÓ?	SI GANÓ, ¿EN CUÁNTOS INTENTOS?	¿CUÁNTAS LETRAS ADIVINÓ?
Zombiz			
Tomate			
Rinoceronte			
3Er3i#u3			

Antes de pasar a la cuarta palabra del juego, decile que ahora se pueden poner expresiones con letras, números y símbolos en lugar de palabras.

En la tabla pusimos un ejemplo, 3Er3i#u3, que obtuvimos utilizando la fábrica de contraseñas seguras.

1. Elegimos la frase: "Por el río Paraná iba navegando un piojo".
2. Anotamos cada una de las iniciales de las palabras, una al lado de la otra: perpinup.
3. Sustituimos letras por números. Por ejemplo, la letra p por el número 3 y la n por el símbolo #. Ahora nuestra frase quedó así: 3er3i#u3.
4. Colocamos en mayúscula al menos una letra, en este ejemplo, la E. Esto nos da: 3Er3i#u3.

¡Vos podés usar otra frase! Dale varias oportunidades a tu familiar para que adivine. Si termina ahorcado, dale más chances. Al finalizar el juego, contale la importancia de elegir contraseñas seguras. Compartí con él las reglas aplicadas a la frase y explicale cómo funciona la fábrica de contraseñas seguras para que confirme que una buena contraseña es difícil de adivinar.

CONTRASEÑAS QUE NO

Una de las contraseñas más usadas es **qwerty**. Esta no es una contraseña segura. ¿Se te ocurre por qué tanta gente la usa? Ayuda: intentá escribirla en el teclado de tu computadora. Otras contraseñas muy inseguras son: **contraseña**, **1234**, **1111**, **123456**, **12345678**. Si una contraseña es muy usada, es probable que sea insegura.[2]

[1] Ahorcado (juego), (s.f.). Wikipedia. Obtenido de http://goo.gl/NkQE7a.

[2] No vale copiar: las 25 contraseñas más usadas, (13 de enero de 2017). *Día a Día*. Obtenido de http://goo.gl/cUnv5u.