Programar en casa

<Program.AR/>

NIVEL SECUNDARIO

Introducción a la computación

La Computadora

Representación de la Información

→ **Ciudadanía digital y seguridad**[1]

¿Qué es Program.AR en casa?

Program.AR en casa es una propuesta para que los chicos y chicas de secundaria se acerquen a la programación, el funcionamiento de las redes y las computadoras acompañados por sus familias o docentes.

Cada kit se compone de tres elementos: las fichas que son un conjunto de actividades agrupadas por tema, una guía para los adultos que quieran ayudar a resolver las actividades y una serie de videos dirigidos a estudiantes con las pistas de solución.

¿De qué se trata esta propuesta?

La propuesta de la Ficha ciudadanía digital y seguridad, es mostrar cómo el mundo tecnológico atraviesa cada vez más aspectos de la vida cotidiana, por ejemplo, cuando realizamos videoconferencias con personas en distantes lugares del mundo. Esta nueva realidad impone nuevas reglas de juego, nos enfrenta a nuevos desafíos y nos expone a riesgos sobre los cuales debemos ser conscientes.

En esta ficha encontraremos cinco actividades. En la primera identificamos qué información puede ser sensible y qué podemos publicar en Internet, además tomamos conciencia de algunos de los riesgos a los que nos enfrentamos en el universo digital. En la segunda vemos lo sencillo que resulta encontrar información personal en Internet, y que, a menos que se tomen las precauciones adecuadas, puede permanecer disponible para desconocidos sin que lo sepamos. En la tercera reflexionamos sobre el robo de identidad y aprendemos qué es el abuso informático conocido como phishing -modificación del inglés fishing, que significa "pesca"-. En la cuarta distinguimos entre contraseñas seguras y otras fácilmente vulnerables, además reconocemos características que hacen a la seguridad de una contraseña. En la quinta aprendemos sobre un mecanismo que permite el intercambio seguro de mensajes, que pertenece a la familia de cifrado simétrico; es decir, que requieren que tanto el emisor como el receptor (y solo ellos) conozcan una clave para poder escribir y leer mensajes.

[1] Material extraído del Manual para la Enseñanza de las Ciencias de la Computación en el aula de la Iniciativa Program.AR. Claudia Banchoff Tzancoff; Vanessa Aybar Rosales; Silvina Justia- novich; Vanina Klinkovich; Hernán Czemerinski (2019). Ciencias de la computación para el aula, 2do ciclo secundaria (1st ed.). Buenos Aires, Argentina: Fundación Sadosky.

Fundación SADOSKY <Program.AR/>

http://program.ar/programar-en-casa

CIUDADANÍA DIGITAL Y SEGURIDAD

¿Cómo usar las fichas?

Las fichas de **Program.AR en casa** se pueden: descargar, imprimir y hacer en papel o bien editar en línea. Usando Adobe Acrobat Reader podrán escribir, dibujar o tildar sobre la ficha y luego guardar el archivo para compartirlo en redes o enviarlo por correo electrónico.

La aplicación se puede usar desde el celular o la computadora teniendo instalado el programa gratuito **Adobe Acrobat Reader 2020**.

Descargar Adobe Acrobat Reader

Descarga web para **Windows**.

Descarga web para **Ububtu**.

Descarga para celulares: **Playstore**.
Ver video para instalar en **Android**.

Instalación y uso

Adobe Acrobat Reader para celulares con Android

Adobe Acrobat Reader para computadoras con Windows

Okular para computadoras con sistema operativo Ubuntu

Te recomendamos elegir el dispositivo, instalar el programa, descargar la ficha y proponerle al estudiante que explore las actividades. Una vez que les haya echado un vistazo pueden intentar resolverlas juntos. En caso que les resulten complejas o quieran verificar si van por el buen camino, les sugerimos visualizar los videos de las pistas.

pistas

- ¡Cuidado: riesgo a la vista!
- Lo que publico, ¿quiénes lo ven?
- No quiero ser un pescado
- Contraseñas ¿seguras?
- Claves compartidas

Recomendaciones

- *Citizen Four* o *El cuarto poder* es un documental sobre la denuncia hecha por Edward Snowden sobre el modo en que gobiernos y empresas comparten información digital sensible y personal. *Edward Snowden* es la película de ficción de Oliver Stone sobre el mismo tema.
- La serie *Black Mirror* tiene varios capítulos interesantes sobre este tema.

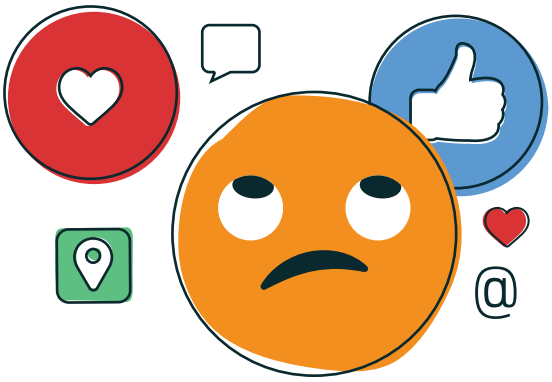
- Si querés conocer todas las guías y fichas entrá acá.
- Si sos docente y querés descargarte el manual original para tus clases podés hacerlo acá:

DESCARGAR MANUAL COMPLETO

NOMBRE Y APELLIDO:

CURSO: FECHA:

¡CUIDADO: RIESGO A LA VISTA!



El desembarco de las redes sociales en nuestras vidas ha modificado el modo de relacionarnos con el mundo. Por ejemplo, hasta hace poco, para mostrarle una foto a un amigo, primero teníamos que imprimirla, luego encontrarnos con él y, finalmente, mirarla juntos. Ahora es mucho más sencillo, ¿no? Este nuevo mundo, más virtual y menos personal, también modificó los riesgos a los que nos exponemos. Frente a nuevas reglas de juego, debemos *aggiornar* las precauciones para no exponernos a situaciones riesgosas.

1. Observá las siguientes publicaciones en redes sociales y respondé las preguntas a continuación.

NOMBRE Y APELLIDO:

CURSO: FECHA:

¿Qué tipo de información brinda cada imagen?

NOMBRE Y APELLIDO:

CURSO: FECHA:

¿Cuáles son los riesgos que podrían originarse a partir de cada una de las situaciones de las imágenes?

En cada caso, ¿la información sensible fue compartida voluntariamente?

2. ¿Tenemos control sobre la información que publicamos en Internet? ¿Por qué?

NOMBRE Y APELLIDO:

CURSO: FECHA:

LO QUE PUBLICO, ¿QUIÉNES LO VEN?

A veces es difícil imaginar hasta dónde puede llegar el contenido que publicamos en Internet. Por suerte, las redes sociales poseen configuraciones de privacidad que nos permiten decidir quiénes pueden ver nuestra información y quiénes no.

1. Contestá las siguientes preguntas, pensando en cada una de las redes sociales y aplicaciones que usás a diario. ¿Conocés la respuesta para todas ellas?

¿Quiénes pueden acceder a la información disponible en tu cuenta?

¿A quiénes aceptás como contactos, amigos, seguidores, etc.?

¿Resultás fácil de encontrar y reconocer? ¿Tu nombre y/o foto de perfil es visible para todos?

¿Quiénes pueden escribirte por *chat*?

NOMBRE Y APELLIDO:

CURSO:

FECHA:

¿Podés bloquear cuentas de desconocidos que intenten contactarte o compartan contenido que te resulta agresivo o desagradable?

¿Cuánta información pueden ver otras personas sobre vos? ¿Todos pueden ver lo mismo?

¿Alguna de las redes sociales que usás se vincula con otras cuentas que uses? ¿Publica automáticamente lo que subís en algún otro sitio? ¿Te pregunta cada vez?

¿Podés ser etiquetado en publicaciones ajenas? ¿Quiénes pueden compartir tus publicaciones?

NOMBRE Y APELLIDO:

CURSO: FECHA:

2. Ingresá a las redes sociales con una cuenta que no forme parte de tus contactos y, una vez adentro, buscá tu nombre y apellido. ¿Con qué te encontraste? ¿Sabías que lo que ves está disponible para cualquier persona? Completá la siguiente tabla con tus hallazgos sobre la privacidad de tus datos en las tres redes sociales que utilices con más frecuencia.

RED SOCIAL	¿QUÉ ENCONTRASTE?	¿SABÍAS QUE ESA INFORMACIÓN ERA ACCESIBLE PARA CUALQUIERA?	¿QUERÉS QUE ESA INFORMACIÓN SEA ACCESIBLE PARA DESCONOCIDOS?

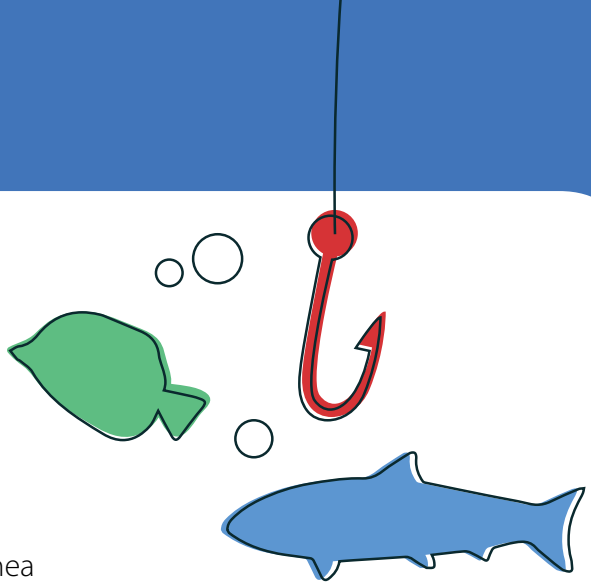
DECIDÍ VOS SOBRE LO PRIVADO Y LO PÚBLICO

Es importante que seas consciente de qué información compartís y con quién. Especialmente, a cuál pueden acceder desconocidos. Si bien las redes sociales permiten configurar el nivel de privacidad de lo que publicás, los niveles por defecto no suelen ser los más restrictivos. Revisá la configuración de tus cuentas y asegurate de que el alcance de tu información no vaya más allá de lo que vos querés.

NOMBRE Y APELLIDO:

CURSO: FECHA:

NO QUIERO SER UN PESCADO



Un pescador pone la carnada en el anzuelo y lanza la línea al agua. Luego, pacientemente esperará hasta que… ¡zaz! ¡El pobre animal mordió el anzuelo! Aunque suene difícil de creer, la pesca virtual existe, y también los pobres pescados.

1. Mirá la siguiente página.

¿Qué es esta página? ¿Para qué se usa?

NOMBRE Y APELLIDO:

CURSO: FECHA:

2. Leé atentamente el siguiente artículo periodístico y respondé las preguntas que se presentan a continuación.[1]

7 de agosto de 2017

25 de mayo: el pueblo al que le robaron $ 3,5 millones con un aviso en Google

Parecía un día más. Un día alegre, en realidad, para este municipio de 40 mil habitantes. Porque en el partido de 25 de mayo, a 220 kilómetros de la Capital, después de mucha insistencia recibían una ambulancia para Norberto de la Riestra, una de las localidades de este partido bonaerense. [...]

La municipalidad

Aquel lunes 21 de noviembre de 2016, Roberto Testa, el tesorero del municipio, entró a trabajar a las 8 de la mañana en 25 de mayo, la ciudad que es cabecera del partido homónimo y que crece junto a la laguna Las Mulitas. A las 10, como todos los días, fue al Banco Provincia. Pidió que le imprimieran un resumen con todos los movimientos de las cuentas bancarias. [...] Ese día detectó, con su ojo prolijo de 32 años de carrera, que algo no andaba bien. "Empiezo y veo en el resumen que teníamos una transferencia por 100 mil pesos, otra por 90 mil. Me fui corriendo a lo del contador a comprobar por qué habíamos hecho esos movimientos", explica. [...]

El *home banking*

Paolo Salinas, el contador hace 18 años y encargado de emitir los pagos, giró su mirada hacia la puerta de la oficina para recibirlo. Escuchó a Testa y de inmediato se metió en las cuentas de *home banking* con su computadora. Salinas es el único que sabe las claves. Y no las anota en ningún lado, "por seguridad", dice. "Están en mi cabeza", acota. [...]

No recuerda específicamente el proceso de ese día, pero por lo general busca "Banco Provincia BIP" (Banca Internet Provincia) en Google, hace clic en el primer resultado, ingresa las claves y empieza a revisar las cuentas. "En ese momento me decía que había un usuario más adentro al mismo tiempo que yo", recuerda. Le preguntó a Romina Mancha, la subcontadora, si era ella. "No", le contestó Mancha desde el otro lado de la oficina, mientras dejaba su silla y se acercaba a la PC de Salinas. [...]

Mancha dejó el monitoreo y fue corriendo hasta la oficina de Ticera, la secretaria de Hacienda, quien a esa hora estaba reunida. No golpeó la puerta cerrada para entrar. "Me interrumpe y me dice: 'nos están robando, nos están robando' [...]", recuerda. [...] Fueron a buscar al Intendente: "Salimos disparadas". [...]

Tres millones y medio

El intendente, de 32 años [...], no salía de su asombro. Le pidió a Salinas que le mostrara lo que estaba sucediendo. Otra vez. Se dieron cuenta de que habían aparecido más transferencias, todas hechas a proveedores no habituales del municipio. "Cada segundo que pasaba perdíamos más plata", rememora. A esa altura, casi el mediodía de ese lunes fatídico, ya había 3 millones y medio menos de pesos en las arcas municipales [...]. Entonces, recibieron al menos una buena noticia: lograron que les bloquearan las cuentas. Eran poco más de las 12. [...]

[1] El artículo completo puede encontrarse en http://bit.ly/2krwGH0.

NOMBRE Y APELLIDO:

CURSO:

FECHA:

Pesca con mediomundo

Juan Ignacio Bidone es fiscal de investigaciones complejas del Departamento Judicial de Mercedes. A esta altura, tiene muy claro lo que pasó. La secuencia del robo de 3 millones y medio pesos al municipio de 25 de mayo, dinero que luego fue extraído de diferentes cuentas, se realizó mediante *phishing*: una forma de engaño informático con la que se logra que un usuario revele información personal. Los ciberdelincuentes crearon un sitio falso similar al de la Banca Internet Provincia, también conocido como BIP por sus iniciales. Era idéntico al verdadero, pero con un detalle: la dirección, que obviamente no puede ser la original. Suplantaron la *a* por la *s*, para hacer más imperceptible el cambio, y montaron un sitio en la dirección bancsprovincia.bancsinternet.com.ar.

El resultado falso que aparecía en Google

Para lograr que alguien visitara ese sitio pensando que estaba entrando al Banco Provincia aplicaron una técnica llamada *black hat SEO*: una estratagema que desafía las reglas para lograr escalar posiciones en los listados de Google. En este caso, contrataron el servicio publicitario de *AdWords*; eso fue determinante, ya que lograron hacer que ante una búsqueda en Google de la frase "Banco Provincia BIP" el sitio falso que crearon apareciera como primer resultado. [...]

Cuando alguien entraba, en el sitio falso se le pedía el nombre de usuario y la clave para ingresar a las cuentas del banco. Capturaba la información y luego redirigía al verdadero sitio BIP para no despertar sospechas. [...] Así —estima la fiscalía— los delincuentes se hicieron de las contraseñas, la única credencial necesaria para realizar la operación. [...]

¿Quién o quiénes fueron las víctimas del ataque descripto en el artículo?

¿Qué información fue robada por el atacante?

NOMBRE Y APELLIDO:

CURSO: FECHA:

¿Para qué fue usada la información robada? ¿Qué consecuencias tuvo el ataque para las víctimas?

¿Cómo se hizo para robar la información de las víctimas? ¿Qué nombre recibe este tipo de ataque?

¿Qué señales podrían haber alertado al contador de que estaba siendo engañado cuando ingresó al sitio web apócrifo?

Escribí otros ejemplos de información que podría ser robada mediante engaños similares.

¿Qué consejos pueden extraer de este artículo para evitar ser víctimas de un ataque como este?

Volvé a mirar la página web de la consigna 1. ¿Te parece que es auténtica?

¿QUÉ ES *PHISHING*?

La palabra *phishing* es una modificación del inglés *fishing*, que significa "pesca", pero reemplazando la letra *f* por la escritura *ph*, recurso que es común en el ambiente *hacker*. Se trata de un abuso informático en el que el perpetrador busca obtener información confidencial acerca de la víctima (por ejemplo, la contraseña de algún servicio o los detalles de su tarjeta de crédito) haciéndose pasar por otra persona, empresa, sitio o entidad en quien la víctima confía, a la manera de un cebo que induce al damnificado a morder el anzuelo y proporcionar la información. Posteriormente, la información robada puede usarse para fines espurios, tales como enviar mensajes a nombre de la otra persona o realizar compras por Internet.

NOMBRE Y APELLIDO:

CURSO: FECHA:

CONTRASEÑAS ¿SEGURAS?

¿Hay contraseñas más seguras que otras? ¿De qué depende su nivel de vulnerabilidad? Acá veremos algunas características de las contraseñas que te van ayudar a saber cuán (in)seguras son las tuyas.

1. A continuación hay una serie de contraseñas que una persona eligió para usar en distintos sitios de Internet. ¿Se te ocurre qué motivos lo llevaron a elegirlas? Completá la tabla.

CONTRASEÑA	POSIBLE MOTIVO PARA HABERLA ELEGIDO
Luis2006	
25062006	
Coco	
D4l3B0c4	
Kpo de Temperley	
Ceci te amo	

¿Te parecen seguras estas contraseñas? ¿Por qué?

CONTRASEÑAS VULNERABLES

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 muy inseguras son: **contraseña**, **1234**, **1111**, **123456**, **12345678**. Si una es muy usada, es probable que sea insegura. En bit.ly/2jZvdY9 podés encontrar las 25 contraseñas más utilizadas durante 2018.

NOMBRE Y APELLIDO:

CURSO: FECHA:

2. Es momento de pensar qué factores contribuyen a la seguridad o vulnerabilidad de las contraseñas. Contestá las siguientes preguntas:

¿Cuántas contraseñas distintas de un dígito pueden existir? ¿Y de dos dígitos?

¿Cuántas contraseñas distintas existen si consideramos que pueden tener tanto un dígito como dos?

¿Y cuántas hay si consideramos que son de una letra del alfabeto castellano? ¿Y si son de dos letras?

¿Qué cantidad de posibles contraseñas hay si permitimos tanto dígitos como letras para contraseñas de longitud 1? ¿Y para contraseñas de longitud 2?

En general, si contamos con *n* símbolos, ¿cuántas combinaciones distintas hay fijando una longitud *l*?

Calculá la cantidad de posibilidades que existe si se pueden usar dígitos, letras en mayúscula y letras en minúscula para contraseñas de 6 símbolos. ¿Son muchas? ¿Cuántas?

FUERZA BRUTA

Hay programas que, para descubrir contraseñas, se valen de la **fuerza bruta**: analizan todas las posibles contraseñas hasta llegar a descubrirla. Si las posibles son relativamente pocas, el programa llegará a probar todas las combinaciones en poco tiempo. ¡Ojo: hablar de millones es muy poco para un computadora! Además, ¿notaste que hay muchos sitios que bloquean el acceso a una cuenta cuando un usuario se equivoca en muchos intentos sucesivos al ingresar su contraseña? Así, evitan ser vulnerados por el uso de esta técnica.

¡ÁBRETE, SÉSAMO!

"Alí Babá y los cuarenta ladrones" es un cuento popular incluido en la célebre recopilación de cuentos árabes medievales *Las mil y una noches*. Alí Babá era un honrado leñador que, sin proponérselo, descubre a una banda de ladrones que esconden los tesoros robados en una cueva cuya boca queda sellada pero que, mágicamente, puede abrirse usando la contraseña "Ábrete, sésamo". Entonces, decide usar la clave a espaldas de los malhechores, para ingresar y llevarse riquezas, de modo que se vuelve también él un saqueador.

NOMBRE Y APELLIDO:

CURSO: FECHA:

CLAVES COMPARTIDAS

La criptografía es un área de la matemática y la computación que se ocupa de desarrollar técnicas que permitan cifrar y descifrar mensajes de modo que, al enviarlos de un lado a otro, pueda preservarse la confidencialidad. Para garantizar que solo el emisor y el receptor comprendan los mensajes, hay técnicas que requieren que ambos compartan una clave (que nadie más conozca). Las técnicas con esta característica se llaman de **cifrado simétrico**.

Uno de los métodos simétricos más antiguos es el de cifrado por sustitución. Para cifrar un mensaje, hay que reemplazar cada letra por otra, siguiendo un criterio solo conocido por el emisor y el receptor. Luego, para descifrarlo, hay que hacer el reemplazo inverso.

A continuación se muestra un posible esquema de reemplazos:

ORIGINAL	A	B	C	D	E	F	G	H	I	J	K	L	M	N
CIFRADO	F	R	J	B	O	X	V	I	D	Z	K	C	W	Q

ORIGINAL	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
CIFRADO	D	S	M	U	A	N	T	G	L	H	Y	E	P

1. ¿Cómo se codifican los siguientes mensajes con el esquema de cifrado propuesto?

CIFRAR MENSAJES → _____

LUCES ESTROBOSCÓPICAS → _____

CUCARACHA → _____

TARTA DE CHOCLO → _____

2. ¡Te llegaron estos mensajes! ¿Qué dicen?

¿UGO MAOTOQBO GNTOB BO WD? → _____

NO CO ONJFMS CF TSATGVF → _____

NOMBRE Y APELLIDO:

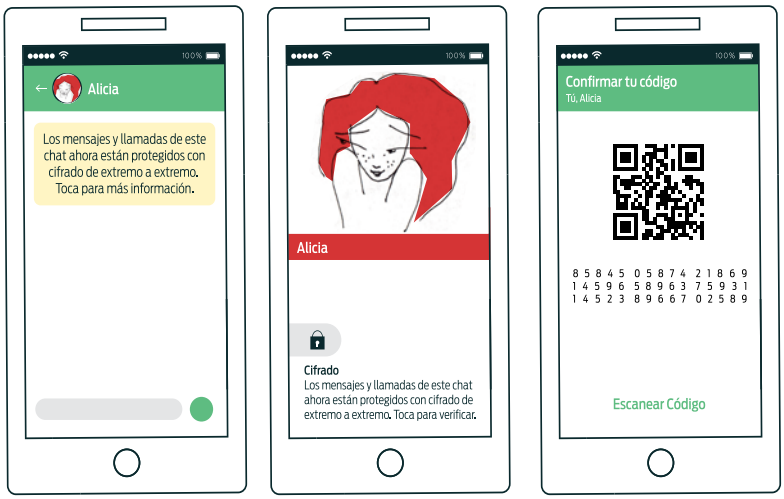
CURSO: FECHA:

JSQ CFN WFQSN CDWMDFN ⟶ _____

CF MOCSTF QS BSRCF ⟶ _____

¿SABÍAS QUE...

… las aplicaciones de mensajería instantánea suelen cifrar los mensajes? Por ejemplo, la primera vez que enviamos un mensaje a un contacto, WhatsApp informa que el intercambio viaja cifrado de extremo a extremo, lo que significa que se cifran en el teléfono del emisor y solo pueden ser descifrados en el teléfono del destinatario.



Entrando a la pantalla de opciones de cualquier contacto y seleccionando la opción "Cifrado", se pueden ver dos representaciones de la clave compartida con ese contacto: como código QR y como una serie de números.

SITIOS SEGUROS

Es sumamente importante que, antes de enviar información sensible a un sitio de Internet (contraseñas, mensajes privados, claves bancarias, etc.), verifiquemos que la comunicación con el sitio esté cifrada.

Cuando usamos un navegador de Internet podemos chequear si la comunicación es segura. En ese caso, en la barra de direcciones aparece un candado y la dirección debería comenzar con "https://", a diferencia de las no seguras, que comienzan con "http://".

Fundación SADOSKY | <Program.AR/>