GOBIERNO DE COLOMBIA

Ruta Grado Séptimo

(7mo) de Secundaria



Sesión 4

Seguridad cibernética

LABORATORIO de Innovación Educativa

OEI

Computadores para Educar

LABORATORIO
de Innovación Educativa



TABLA DE CONTENIDO

Introducción 2
1. Prepara la clase 2
1.1 Recursos de las Nuevas Soluciones Tecnológicas 2
1.2 Espacio de trabajo 2
1.3 Conocimientos previos 2
1.4 Recomendaciones de uso de: las NST, los materiales adicionales y la organización de grupos de trabajo 3
2. Identificación del Contexto y problema para desarrollar 3
2.1 Problemática 3
2.2. Marco Teórico 4
3. Metas de aprendizaje STEM 7
3.1 Ciencias 7
3.2 Tecnología 7
3.3 Matemáticas 7
3.4 Ingeniería 7
3.5 Lenguaje 8
3.6 Matemáticas 8
3.7 Ciencias sociales 8
3.8 Ciencias naturales 8
3.9 Tecnología 8
3.10 Competencia ciudadana 8
4. Desarrollo práctico de la sesión 9
4.1 Objetivo 9
4.2 Aplicación práctica 9
4.3 Gestor de Contenidos 9
4.4 Programación 10
4.5 Construcción 19
4.6 Monitor Interactivo 21
5. Reflexiona, evalúa y concluye 21
5.1 Reflexión y evaluación 22
6. Conclusión 22
7. Bibliografía 22



Introducción

Bienvenidos a la Ruta de Aprendizaje de Grado Séptimo (7mo) de Secundaria, en esta Ruta, encontrará seis (6) sesiones enmarcadas en didácticas que permiten desarrollar en los estudiantes habilidades de Programación Básica, Pensamiento Computacional y trabajo colaborativo para la resolución de problemáticas planteadas en situaciones cotidianas y científicas.

A través de la Metodología Aprendizaje basado en problemas (ABP) y el uso básico de la tarjeta micro:bit, se busca gestionar proyectos tecnológicos incluyendo el uso de herramientas que hacen parte de las Nuevas Soluciones Tecnológicas (de ahora en adelante, NST) como: la impresora 3D, monitor interactivo, gestor de contenidos y elementos adicionales didácticos; en donde los docentes y estudiantes podrán desarrollar actividades relacionadas con STEM (Ciencia, Tecnología, Ingeniería y Matemáticas).

1. Prepara la clase

1.1 Recursos de las Nuevas Soluciones Tecnológicas

En esta segunda sesión, se usarán los siguientes recursos de las NST:

- Kit de Ingeniería STEM.
- Monitor interactivo.
- Gestor de contenidos.

1.2 Espacio de trabajo

Organizar el salón de clase para que se pueda desarrollar la dinámica en grupos de a cinco (5) estudiantes que permitirá realizar el trabajo colaborativo y la división de roles propuesta.

1.3 Conocimientos previos

Se recomienda identificar y generar en los estudiantes los siguientes conocimientos previos para el desarrollo de esta sesión:

- Claves seguras
- Protección de datos
- Seguridad en la web





1.4 Recomendaciones de uso de: las NST, los materiales adicionales y la organización de grupos de trabajo

Para el desarrollo de esta sesión se recomienda verificar el correcto funcionamiento de las NST que se van a utilizar y también los materiales adicionales señalados.

Por otro lado, para fomentar el trabajo colaborativo, se recomienda asignar a los estudiantes los siguientes roles basados en Liderazgo, Ingeniería y Programación.

La descripción de las labores de cada grupo es:

Líder (2): Son los encargados de organizar, supervisar y encontrar soluciones para posibles problemáticas que se puedan presentar en el desarrollo de la actividad, ellos se encargaran de apoyar al equipo de programadores para visualizar el correcto funcionamiento del prototipo propuesto en esta sesión.

Ingeniero (2): son los encargados de construir con las fichas de armar una estructura que simule un celular en donde va incluido la tarjeta micro:bit de bloqueo y desbloqueo.

Programador (4): son los encargados de programar los algoritmos para las dos tarjetas micro:bit para el correcto funcionamiento, una vez que se le haya integrado toda la parte electrónica y de programación.

2. Identificación del Contexto y problema para desarrollar

2.1 Problemática

Actualmente la Seguridad Cibernética es muy importante debido a la gran cantidad de datos personales que la mayoría de las personas del mundo tiene guardada en internet. Por ejemplo: datos bancarios, correos electrónicos, fotos personales, redes sociales y mucho más. Por esa razón, es muy importante aprender sobre buenas prácticas digitales y entre otras cosas, eso incluye proteger nuestros datos con la creación de contraseñas seguras. En un Centro de Tecnología itinerante se está dando la información necesaria para que las personas aprendan a crear contraseñas seguras y valoren la importancia de esta para

la seguridad de sus datos. En este caso, para demostrar cómo funcionan las contraseñas en un sistema, deciden crear un experimento donde se muestra la lógica en la programación de una contraseña. Seamos parte de este taller y aprendamos a más profundidad cómo funcionan las contraseñas en el mundo digital que cada vez hace parte de nuestras vidas.

2.2. Marco Teórico

¿Qué es el Phishing?

El phishing se refiere al envío de correos electrónicos que tienen la apariencia de proceder de fuentes de confianza (como bancos, compañías de energía etc.) pero que en realidad pretenden manipular al receptor para robar información confidencial. Por eso siempre es recomendable acceder a las páginas web escribiendo la dirección directamente en el navegador.

Cómo actúa el Phishing

La mayoría de los ataques de phishing comienzan con la recepción de un correo electrónico o un mensaje directo en el que el remitente se hace pasar por un banco, una empresa u otra organización real con el fin de engañar al destinatario. Este correo electrónico incluye enlaces a un sitio web preparado por los criminales -que imita al de la empresa legítima- y en el que se invita a la víctima a introducir sus datos personales.

En este sentido existe una vinculación entre el spam y el phishing, ya que los correos electrónicos fraudulentos suelen enviarse de forma masiva para multiplicar el número de víctimas potenciales de los hackers. De hecho, si bien el e-mail continúa siendo el medio más utilizado por los ciberdelincuentes para este tipo de fraudes, el phishing puede utilizar otros medios de comunicación, además: son frecuentes los intentos vía SMS (a veces llamados smishing), VoIP (vishing) o los mensajes instantáneos en redes sociales.

Además, los criminales se valen de ciertos trucos de ingeniería social para crear alarma en los receptores de los mensajes, con indicaciones de urgencia, alarma y diferentes llamadas a la acción. La idea es que el usuario actúe de inmediato ante el estímulo y no se detenga a analizar los riesgos de su acción.

Cómo reconocer un mensaje de Phishing

Es raro que las empresas ya sean de banca, energía o telecomunicaciones- pidan datos personales vía correo electrónico. El mero hecho de que ocurra debería ponernos en guardia.

No siempre es fácil reconocer los mensajes de phishing por su apariencia. Sin embargo reproducir de manera fidedigna el formato de una empresa requiere un tiempo y esfuerzo que los criminales no suelen estar dispuestos a invertir. Los errores, incoherencias o faltas de ortografía son un indicio claro. Fíjate también en la dirección del remitente.

Sé precavido en las operaciones desde tu smartphone. La creciente popularidad de los teléfonos inteligentes hace que muchos usuarios realicen muchas de sus gestiones en su móvil. Los criminales lo saben y tratan de aprovecharse de la pérdida de claridad derivada de pantallas más pequeñas y de menores medidas de seguridad.

Cómo protegerse contra el Phishing

Después de leer el correo no hagas clic en ningún enlace. Realiza las verificaciones pertinentes en tu espacio personal de cliente, acudiendo directamente desde la Url del navegador.

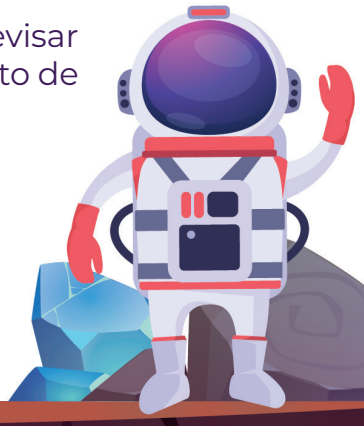
Mejora la seguridad de su ordenador. El sentido común y el buen juicio son tan vitales como mantener tu equipo protegido, pero además, siempre debes tener las actualizaciones más recientes de tu sistema operativo y navegador web.

Además, lo ideal es que cuentes con una capa adicional con un antivirus profesional.

Introduce tus datos confidenciales sólo en sitios web seguros. Para que un sitio se pueda considerar como ‘seguro’, el primer paso -aunque no el único- es que empiece por “https://”, lo que implica que sigue el protocolo de transferencia de hipertexto, y que el navegador muestre el icono de un candado cerrado.

Revisa periódicamente tus cuentas. Nunca está de más revisar facturas y cuentas bancarias cada cierto tiempo para estar al tanto de cualquier irregularidad en las transacciones.





Ante cualquier duda, no te arriesgues. El mejor consejo ante el phishing es siempre fomentar la prudencia entre todas las personas que forman parte de la organización. Asegurar la autenticidad del contenido ante la más mínima sospecha es la mejor política.

Panda a WatchGuard brand. (13 de octubre de 2022). Revenge Porn: definición. Pandasecurity.com. https://www.pandasecurity.com/es/security-info/revenge-porn/

Definición de robo de datos

El robo de datos, también conocido como robo de información, es la transferencia o el almacenamiento ilegal de información personal, confidencial o financiera. Esto podría incluir contraseñas, códigos de software o algoritmos, y procesos o tecnologías patentadas. El robo de datos se considera una vulneración grave de la seguridad y la privacidad que tiene consecuencias potencialmente graves para las personas y las organizaciones.

¿Qué es el robo de datos?

El robo de datos es el acto de robar información digital almacenada en equipos, servidores o dispositivos electrónicos para obtener información confidencial o afectar la privacidad. Los datos robados pueden incluir información de una cuenta bancaria, contraseñas de Internet, números de pasaporte, números de licencias de conducir, números de seguro social, historias clínicas, suscripciones de Internet, etc. Una vez que una persona no autorizada tiene acceso a información personal o financiera, puede eliminar, modificar o impedir el acceso a esta sin el permiso del propietario.

El robo de datos suele ocurrir debido a que los criminales desean vender la información o usarla para el robo de identidad. Si los ladrones de datos roban suficiente información, pueden usarla para acceder a cuentas seguras, generar tarjetas de crédito con el nombre de la víctima o usar su identidad para beneficiarse de algún modo. El robo de datos solía ser un problema principalmente para las empresas y organizaciones, pero, desafortunadamente, es un problema cada vez más usual para las personas.

Aunque el término hace referencia a un “robo”, el robo de datos no significa necesariamente que se le quita la información a la víctima. En cambio, en un robo de datos, el atacante simplemente copia o duplica la información para su propio uso.

Los términos “vulneración de datos” y “filtración de datos” pueden usarse indistintamente cuando se hace referencia al robo de datos. Sin embargo, son diferentes:

Una filtración de datos ocurre cuando se exponen datos confidenciales por accidente, ya sea en Internet o a través de dispositivos o discos duros perdidos. Esto permite que los ciberdelincuentes obtengan acceso no autorizado a datos confidenciales sin esfuerzo de su parte.
Por el contrario, una vulneración de datos hace referencia a ciberataques intencionales.

Kaspersky. (13 de octubre de 2022). ¿Qué es el robo de datos y cómo evitarlo? Latam.kaspersky.com. https://latam.kaspersky.com/resource-center/threats/data-theft

3. Metas de aprendizaje STEM

3.1 Ciencias

Indago sobre ciberseguridad y reflexiono sobre ello.

3.2 Tecnología

Emplear herramientas tecnológicas para el desarrollo de un sistema de seguridad para evitar robos.

3.3 Matemáticas

Calcula diferentes lógicas para la creación de algoritmos.

3.4 Ingeniería

Crea un prototipo que cumpla con la simulación de un celular en donde este integrada la tarjeta micro:bit para generar contraseñas.





Metas establecidas por el Ministerio de Educación Colombiano

Adicionalmente, durante el desarrollo práctico de esta sesión, se busca que los estudiantes cumplan con las siguientes metas de aprendizaje establecidas por el Ministerio de Educación Colombiano:

3.5 Lenguaje

Comprendo el concepto de coherencia y distingo entre coherencia local y global, en textos míos o de mis compañeros.

3.6 Matemáticas

Conjeturo acerca del resultado de un experimento aleatorio usando proporcionalidad y nociones básicas de probabilidad.

3.7 Ciencias sociales

Clasifico las fuentes que utiliza (en primarias o secundarias, y en orales, escritas, iconográficas, estadísticas).

3.8 Ciencias naturales

Identifico y verifico condiciones que influyen en los resultados de un experimento y que pueden permanecer constantes o cambiar (variables).

3.9 Tecnología

Diseño programas digitales que permitan dar solución a los problemas propuestos en contextos de la informática, la cibernética, la robótica o la domótica.

3.10 Competencia ciudadana

Describo casos en los que la evolución de las ciencias ha permitido optimizar algunas de las soluciones tecnológicas existentes.





4. Desarrollo práctico de la sesión

4.1 Objetivo

Sensibilizar a los estudiantes sobre la ciberseguridad haciendo uso de contraseñas confiables mediante el uso de las tarjetas micro:bit.

4.2 Aplicación práctica

Resumen de la actividad

En esta actividad los estudiantes con las fichas de ingeniería del Kit STEM deberán, construir un prototipo de celular para simular el bloqueo y desbloqueo del mismo con las contraseñas programadas en la tarjeta micro:bit.

Para la aplicación práctica de esta sesión se describirán los pasos a seguir para el uso de la siguientes NST:

4.3 Gestor de Contenidos

¿Qué es el Gestor de Contenidos?

El Gestor de Contenidos es un repositorio de recursos educativos que genera una red inalámbrica con ayuda de un router al que se encuentra conectado para permitir la conexión de hasta 45 dispositivos externos como computadoras, celulares y tabletas, los cuales pueden acceder al Gestor para explorar, visualizar y descargar sus contenidos y generar un correcto desarrollo de las sesiones. Este sistema trabaja completamente Offline (desconectado) y le entregará al docente todos los recursos que necesitará para las sesiones.

En el Gestor de Contenidos se aloja todo el material digital necesario para el correcto desarrollo de esta sesión. Encontraremos en él:

- Esta sesión en formato PDF.
- También encontráremos vídeos relacionados con los conceptos requeridos de esta sesión de esta manera se busca que el docente exponga al estudiante de una manera visual conceptos que son necesarios para el desarrollo de esta sesión. Los videos sugeridos son los siguientes:

- Cómo evitar el Phishing
- Conceptos básicos sobre seguridad informática
- La ruta para encontrar los videos en el Gestor de Contenidos es:

Repositorio Recursos Rutas CPE. Fase II – Ruta 7–Sesión3- Videos didácticos

4.4 Programación

¿Qué es la micro:bit?

La micro:bit es una tarjeta programable de 4x5cm que se puede programar mediante lenguaje de bloques y utilizarse en todo tipo de aplicaciones tecnológicas, ya sea sola o conectada a otras micro:bit, acompañada de cables tipo caimán y hojas de papel aluminio, o conectada a todo tipo de sensores y robots.

Esta tarjeta cuenta con una matriz LED de 5x5 LEDs, 2 botones programables, un parlante y un amplio conjunto de sensores integrados que se pueden programar para usarse en cualquier aplicación, como un acelerómetro, un micrófono, un sensor de luz, un sensor de temperatura, una brújula, un sensor touch y un conjunto de hasta 20 pines de entrada y salida digitales y analógicos.

MakeCode

¿Qué es MakeCode?

MakeCode es una plataforma de programación web que se puede abrir desde cualquier navegador donde se utiliza un método de programación por bloques para construir los algoritmos que se descargarán en la micro:bit con el fin de realizar alguna actividad tecnológica. Los bloques tienen diferentes formas geométricas que determinan cómo se conectan, están organizados por categorías y la mayoría de ellos están traducidos al español. La plataforma también cuenta con un emulador de la micro:bit donde se pueden probar todos los algoritmos antes de descargarlos en la tarjeta.

Adicionalmente, si se trabaja MakeCode en el navegador Google Chrome actualizado, es posible conectar la tarjeta al navegador ya sea para visualizar la lectura de sus sensores o los datos que se deseen mostrar en el monitor serial, o para programarla directamente con un solo clic.

En esta sesión se usará las dos tarjetas micro:bit y la plataforma de programación MakeCode para realizar dos algoritmos que cumplan con las siguientes tareas:

Tarjeta microbit contraseña:

- Al presionar el botón A genera números del 0 al 99 al azar.
- Al presionar el botón B se genera una variable llamada “contraseña” donde se le asigna un valor numérico y esos valores representan un símbolo que se utiliza para generar la contraseña.

Tarjeta micro:bit Bloqueo y desbloqueo:

- Al presionar el botón A muestra una cadena desbloqueo, más los 3 dígitos de la contraseña.
- Al presionar el botón B muestra una cadena desbloqueo, uena una nota musical y se apagan los LEDs.

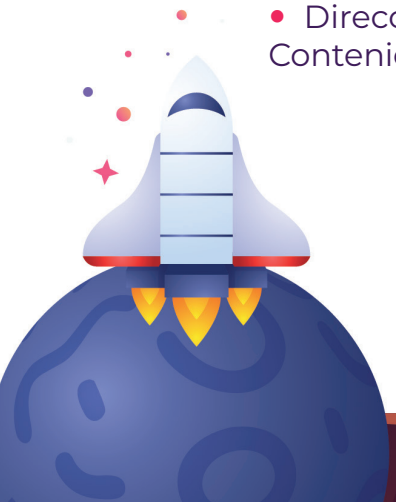
Tenga en cuenta las siguientes recomendaciones antes de iniciar la programación:

- Para ingresar a MakeCode debe escribir el siguiente link en el buscador (preferiblemente Google Chrome), o instalar y abrir MakeCode Offline en el dispositivo donde se vaya a trabajar (el instalador se encuentra en el Gestor de Contenidos)

- Dirección URL de MakeCode: ***https://makecode.microbit.org/***
- Dirección en el Gestor de Contenidos de la aplicación MakeCode Offline: ***Repositorio Técnico NST. Fase II- Instaladores.***

- Para resolver cualquier duda o inquietud sobre los bloques de programación, el correcto uso de MakeCode y micro:bit, o la conexión de los elementos electrónicos, puede remitirse al Manual del Kit de Ingeniería STEM en la sección de “Software” o “Hardware” según corresponda.

- Dirección de Manual del Kit de Ingeniería STEM en el Gestor de Contenidos: ***Repositorio Técnico NST. Fase II- Manuales.***
- Dirección del Manual del Kit de Ingeniería STEM en el Gestor de Contenidos:***KitdeIngenieríaSTEM>ManualdelKitdeIngenieríaSTEM.***





- Para usar las librerías necesarias en los algoritmos propuestos, recuerde cargar la librería que se encuentra en el Gestor de Contenidos, siguiendo los pasos que se describen en el Manual del Kit de Ingeniería STEM.

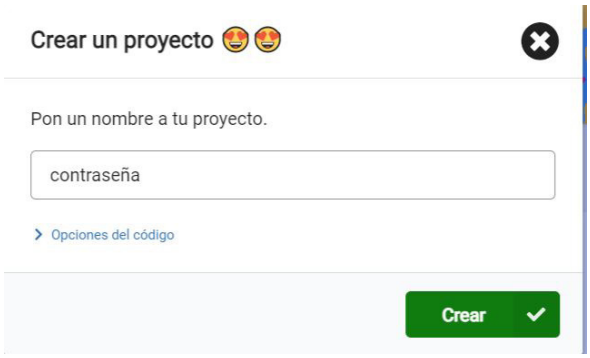
- Dirección de las librerías en el Gestor de Contenidos: ***Repositorio Técnico NST. Fase II – Librerías***
- Dirección del Manual del Kit de Ingeniería STEM en el Gestor de Contenidos: ***Repositorio Técnico NST. Fase II – Manuales***

- Si presenta dificultades para programar el algoritmo propuesto, puede descargarlo del Gestor de Contenidos en la siguiente dirección. Recuerde que estos algoritmos puede cargarlos a MakeCode si los quiere ver, editar o simular, o descargarlos directamente en la micro:bit:

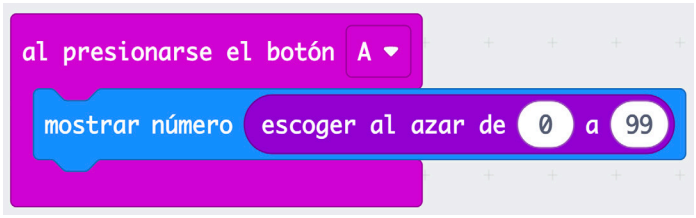
- ***Repositorio Recursos Rutas CPE. Fase II – Ruta 7– Sesión 4 -Micro:bit***

Tarjeta microbit contraseña:

1. Crea un nuevo proyecto y defínele un nombre, por ejemplo, “contraseña”



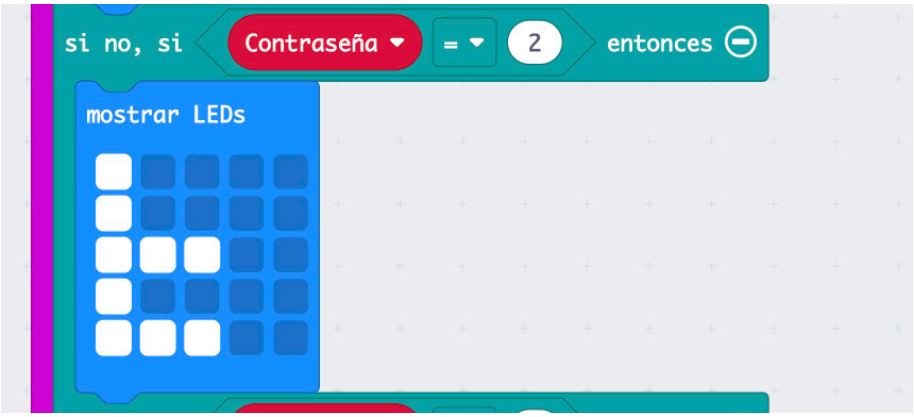
2. Agrega en el bloque “Al presionar el botón A” que se encuentra en la categoría “entrada”, seguidamente agrega el bloque “mostrar número” que se encuentra en la categoría “básico”, agrega el el (0) el bloque “escoger al azar” y cambia los valores numéricos por (0) a (99)



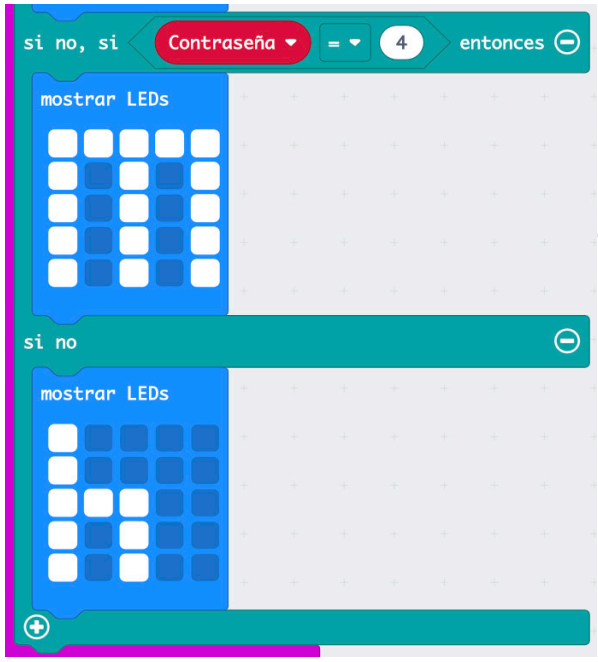
3. Agrega el bloque “al presionar el botón B”, que se encuentra en la categoría “entrada”, crea una variable “contraseña”, y agrega el bloque “establecer contraseña para..” que se encuentra en la categoría “variables” duplica con click derecho el bloque “escoger al azar de 0 a 99” y agrégalo, agrega el bloque “si, verdadero, entonces” que se encuentra en la categoría de “lógica”, agrega el bloque (0=0) que se encuentra en la categoría “lógica” agrega “contraseña” y cambia el valor numérico a 1, finalmente agrega el bloque mostrar icono y elige la X.



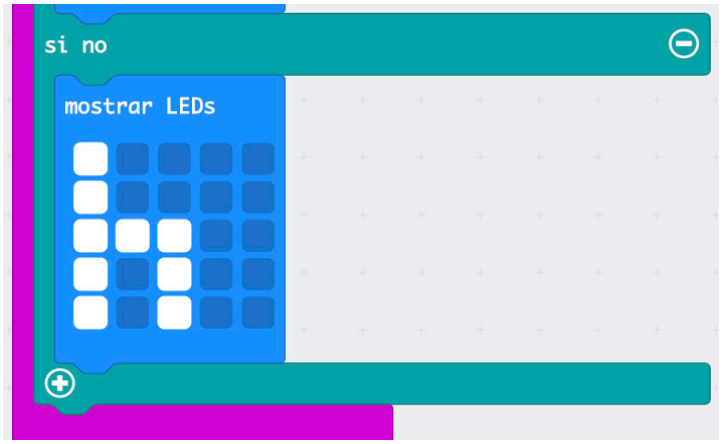
4. Agrega el bloque “si, no si, verdadero entonces...” que se encuentra en la categoría “lógica” agrega el bloque (0=0) y cambia los valores por “contraseña y 2”, agrega el bloque mostrar LEDs y dibuja algo similar.



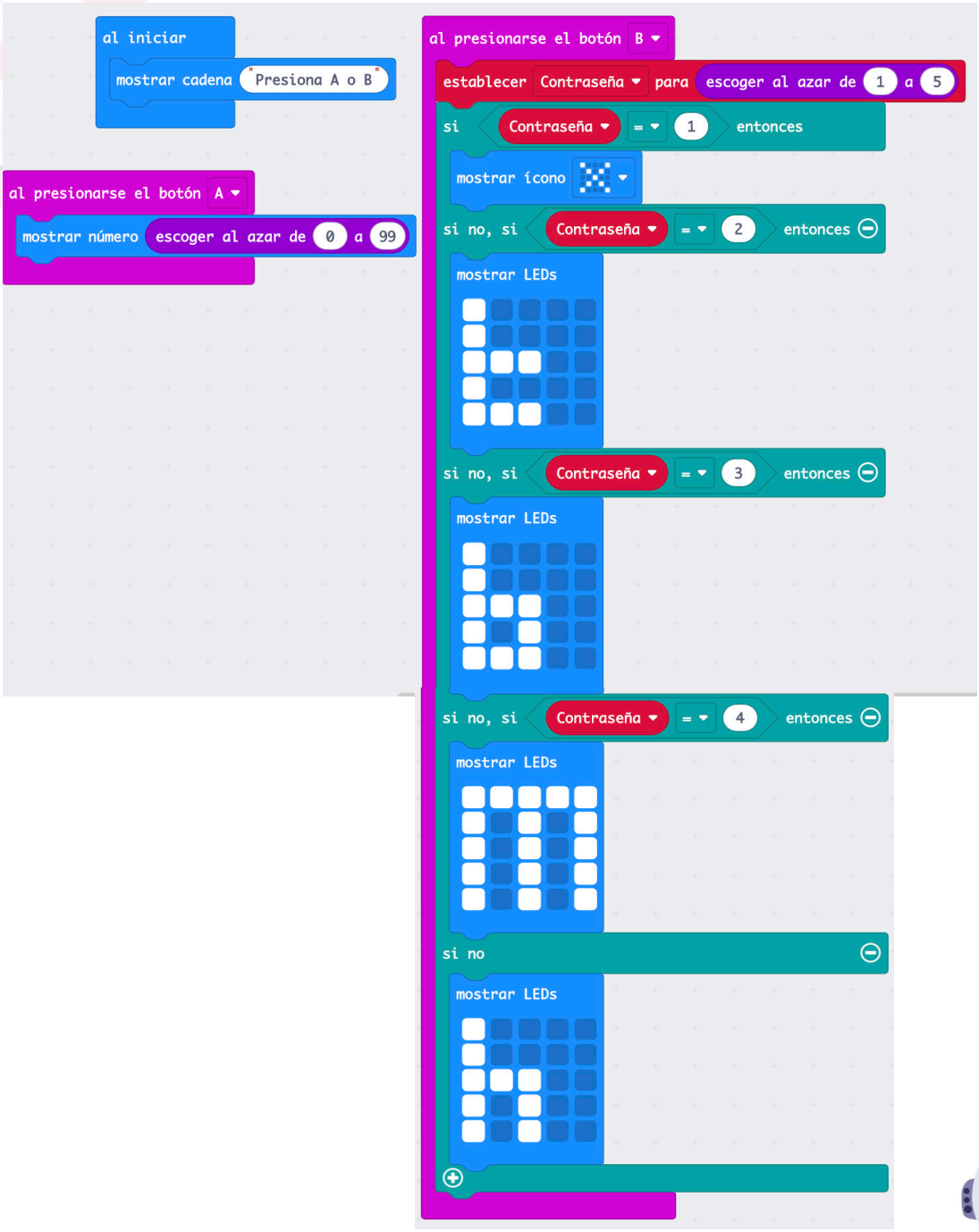
5. Agrega un nuevo condicional “si verdadero entonces...” y agrega el bloque de lógica (0=0) y cambia los valores por “contraseña y 3”, bloque mostrar LEDs y dibuja algo similar.



6. Agrega un nuevo condicional “si, no...” y mostrar LEDs y dibuja algo similar.

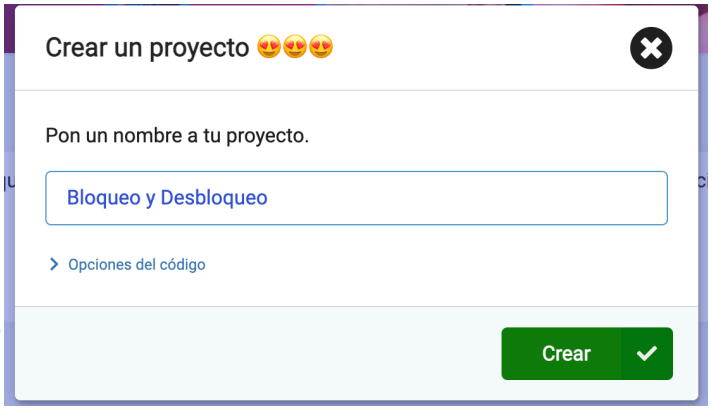


A continuación, se muestra el algoritmo de la programación como debe quedar:

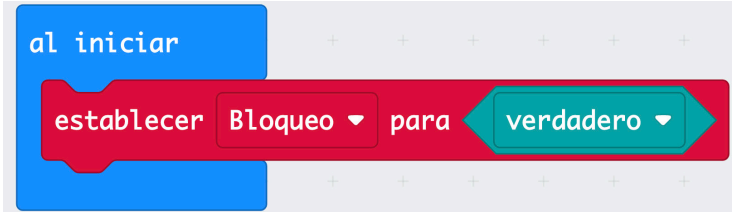


Tarjeta micro:bit Bloqueo y desbloqueo:

1. Crea un nuevo proyecto y defínele un nombre, por ejemplo, “Bloqueo y des-bloqueo”



2. Agrega en el bloque al iniciar una nueva variable “Bloqueo” y agrega el bloque “establecer bloqueo “ este se encuentra en la categoría “variables” agrega el bloque “verdadero” que se encuentra en la categoría ”lógica” .



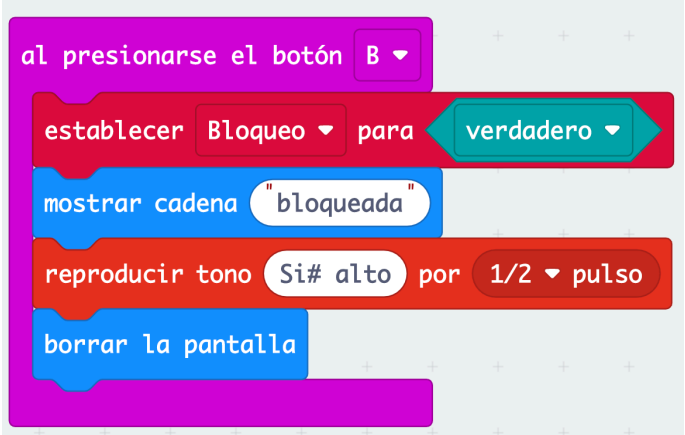
3. Agrega en el bloque para siempre, el bloque “si verdadero, entonces..” que se encuentra en la categoría “lógica”, agrega el bloque () y () que se encuentra en la categoría lógica “boleano”, en el primer recuadro agrega el bloque (0=0) que está en la categoría de “lógica”, cambia los valores, “bloqueo = Verdadero” agrega el bloque, Botón A presionado, que se encuentra en la categoría “entrada”, agrega el bloque “mostrar cadena” escribe, Desbloqueada, agrega el bloque “establecer bloqueo para falso” que se encuentra en la categoría “variables”



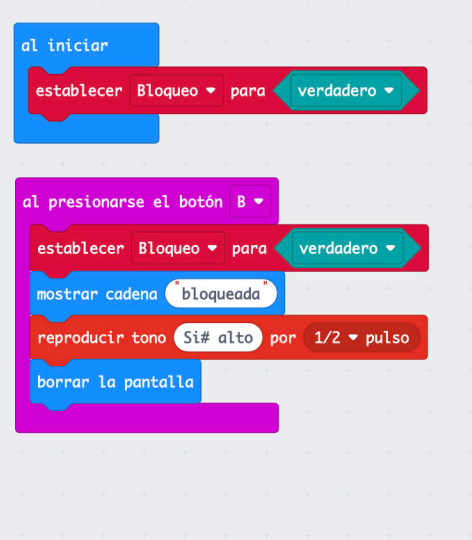
4. Agrega el bloque “si, bloqueo= falso, entonces”, mostrar número (se escribe el que le salió en la contraseña + el icono) agrega el bloque “pausa 1000

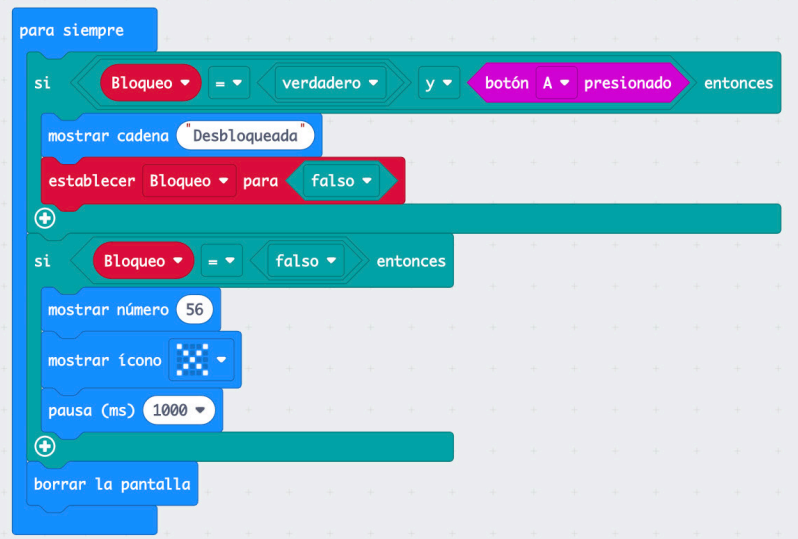


5. Agrega el bloque “al presionar el botón B” que se encuentra en la categoría “entrada”, agrega el bloque “establecer Bloqueo para Verdadero” que se encuentra en la categoría “variables”, agrega el bloque mostrar cadena, escribe (bloqueada), agrega el bloque “reproducir tono si alto po ½ pulso” que se encuentra en la categoría “música”, agrega el bloque “borrar pantalla” que se encuentra en la categoría “básico”.



A continuación se muestra el algoritmo como debe quedar:





Para simular la actividad propuesta en esta sesión, asegúrese de tener abierto el proyecto realizado en MakeCode e interactúe con el emulador de la tarjeta micro:bit como se menciona a continuación:

Tarjeta microbit contraseña:

- Al presionar el botón A genera números del 0 al 99 al azar.
- Al presionar el botón B se genera una variable llamada “contraseña” donde se le asigna un valor numérico y esos valores representan un símbolo que se utiliza para generar la contraseña.

Tarjeta micro:bit Bloqueo y desbloqueo:

- Al presionar el botón A muestra una cadena desbloqueo, más los 3 dígitos de la contraseña.
- Al presionar B muestra una cadena de bloqueo, suena una nota musical y se apagan los LEDs.

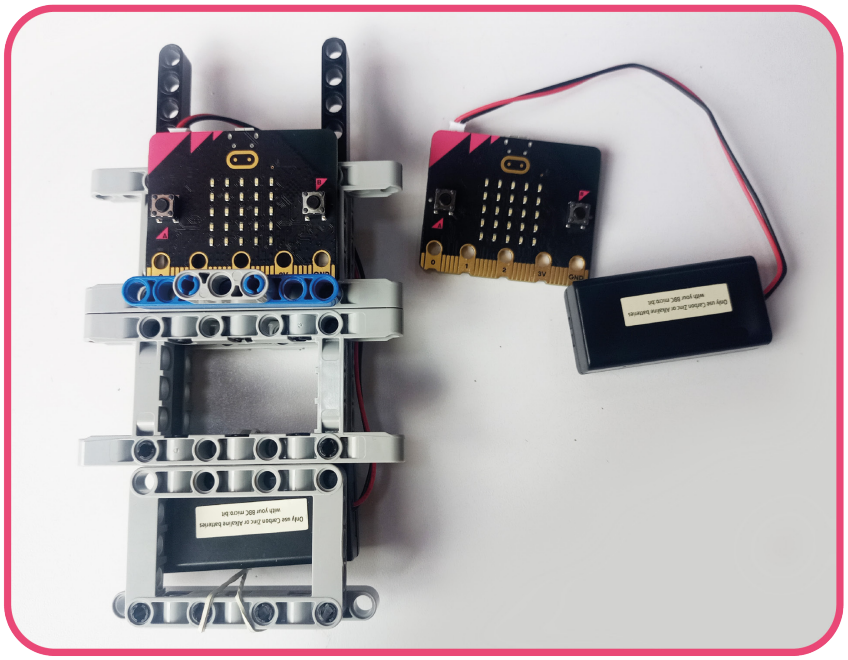
Después de probar la actividad en el emulador, conecte el micro:bit al computador y descargue el programa en la tarjeta, como se indica en el Manual del Kit de Ingeniería STEM. Asegúrese de programar cada micro:bit con el algoritmo correspondiente.

4.5 Construcción

Para el correcto desarrollo de esta actividad, es necesario que se realice la siguiente estructura con el fin de realizar un soporte para la tarjeta micro:bit que simule un celular, para ello tenga en cuenta los siguientes elementos:

- Bloques de ingeniería
- 2 Tarjeta micro:bit

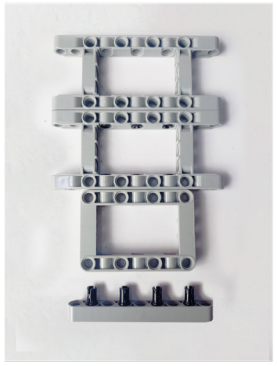
Prototipo celular



Los pasos para ensamblar celular con la tarjeta micro:bit se muestran a continuación. Recuerde que estas imágenes y esta estructura son solo una guía para el correcto desarrollo de la práctica, los estudiantes tienen completa libertad para armar otra estructura o modificar la propuesta en este documento, siempre y cuando dé solución a la problemática indicada en esta sesión:

PASOS DE ENSAMBLE

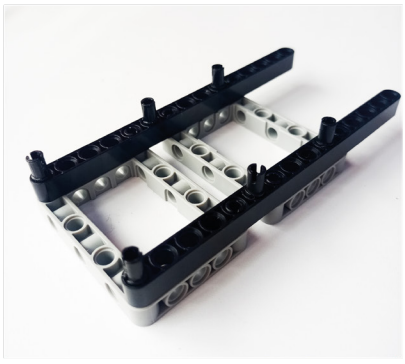
1



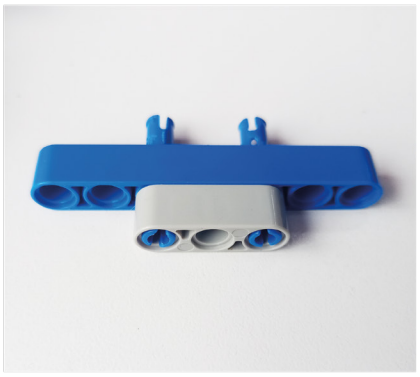
2



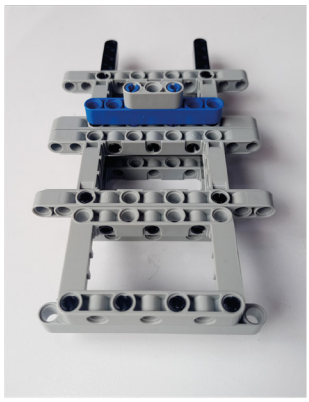
3



4



5



4.6 Monitor Interactivo

¿Qué es el Monitor Interactivo?

El Monitor Interactivo es una pantalla táctil que está conectada al Gestor de Contenidos y permite mostrarles a los estudiantes los archivos almacenados del Gestor, los cuales incluyen el PDF de la sesión, videos imágenes y demás. Adicionalmente, su componente táctil le permite al docente invitar a los estudiantes a interactuar con los contenidos presentados en el monitor, editarlos, moverlos, rayarlos o dibujar nuevos elementos para expresar sus ideas, resolver un problema o mostrar algo relevante a la clase.

En esta sesión, se usará el monitor interactivo para que el estudiante mediante el simulador MakeCode realice las contraseñas dentro de la tarjeta micro:bit de bloque y desbloqueo, así mismo para visualizar los videos propuestos en esta sesión.

Recuerda que el simulador de MakeCode Offline se encuentra dentro del Gestor de Contenidos: ***Repositorio Técnico NST. Fase II- Instaladores.***

5. Reflexiona, evalúa y concluye

5.1 Reflexión y evaluación

Se sugiere que el docente realice las siguientes actividades de evaluación y conclusión con los estudiantes:

Realice las siguientes preguntas:

- ¿Por qué es importante cambiar frecuentemente las contraseñas?
- ¿Qué es Phishing?
- ¿logramos desbloquear el simulador del celular?





6. Conclusión

En esta sesión, los estudiantes tuvieron la oportunidad de conocer y comprender la importancia de la ciberseguridad, ya que en este siglo todo lo hacemos mediante la web.

Finalmente, lograron combinar sus habilidades de construcción y programación para desarrollar el prototipo del celular, cumpliendo con la funcionalidad de alternar contraseñas al azar y generar un bloqueo y desbloqueo de la tarjeta micro:bit.

7. Bibliografía

- Panda a WatchGuard brand. (13 de octubre de 2022). Revenge Porn: definición. Pandasecurity.com. ***https://www.pandasecurity.com/es/security-info/revenge-porn/***

- Kaspersky. (13 de octubre de 2022). ¿Qué es el robo de datos y cómo evitarlo? Latam.kaspersky.com. ***https://latam.kaspersky.com/resource-center/threats/data-theft***



