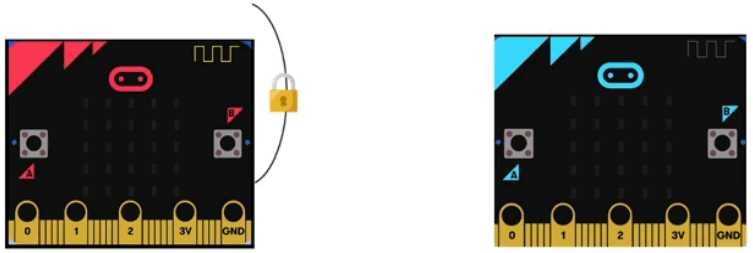
Ceibal | Pensamiento Computacional e Inteligencia Artificial

Cripto:bit

Criptografía en la vida cotidiana

La formación de la ciudadanía es un proceso complejo que se entrelaza con acciones cotidianas y el conocimiento de elementos que se ponen en juego al interactuar con los demás miembros de la sociedad. Un ciudadano pleno tiene derecho a comprender el funcionamiento y el sentido de las tecnologías que impactan en el quehacer de todos los días.

Este proyecto invita a los estudiantes a experimentar el transporte de datos utilizando las placas micro:bit para poner en evidencia la vulnerabilidad de los datos transportados sin cifrar. El recorrido práctico se completa con situaciones de codificación y decodificación orientadas a comprender cómo funcionan las tecnologías que posibilitan una comunicación segura en nuestra sociedad, destacando la importancia de la protección de los datos en una época en la que estos circulan masivamente.



Duración: 3 a 4 semanas.

Materiales: Placa micro:bit.

Índice

Ficha Curricular ↓

Objetivos de aprendizaje de 2º año de Pensamiento Computacional

Comunicación y Colaboración
- Participar de forma proactiva en un proyecto grupal.

Computación, sociedad y equidad
- Conocer y experimentar que se puede utilizar las computadoras para extraer información variada a partir de un conjunto de datos.
- Comprender que ciertos problemas sociales del entorno pueden ser abordados desde una perspectiva computacional.
- Reflexionar sobre la seguridad de los datos compartidos en una red.

Evaluación
-Identificar y corregir, con ayuda del docente, errores mediante un proceso sistemático.

Contenidos PC:
●Cifrado ● Comunicación inalámbrica

Perspectiva de género
Propiciar una experiencia educativa inclusiva y promotora de equidad de género que desnaturalice en forma constante el sesgo de la computación como tarea exclusiva de varones. Buscamos incentivar el trabajo de las niñas y brindarles las herramientas necesarias (atención, apoyo, retroalimentación positiva, entre otras).

Referencias al Marco Curricular Nacional

Espacio Técnico - Tecnológico. Unidad curricular Ciencias de la Computación y Tecnología Educativa. Tramo 4

Competencias generales

Comunicación, Pensamiento Computacional, Pensamiento Crítico, Ciudadanía local, global y digital.

Competencias específicas	Contenidos específicos
CE2 Busca, analiza y selecciona información pertinente, para utilizarla de acuerdo a sus necesidades y reflexionar sobre los criterios de validez y fiabilidad. CE3 Identifica algunas formas en las que la tecnología impacta en la vida cotidiana y el ambiente, permitiéndole adoptar una actitud crítica y ética. CE7 Identifica hechos y situaciones potencialmente riesgosos y utiliza de forma segura y responsable, con mediación, los espacios digitales y las tecnologías de la información, en distintos ámbitos de la vida cotidiana.	Oportunidades y desafíos vinculados a las tecnologías digitales tanto en los entornos locales como en los globales (gestión de grandes volúmenes de datos —big data—, ciberseguridad y redes sociales; realidad virtual y aumentada, entre otros). Internet como conjunto de redes interconectadas para la comunicación y el intercambio de información a través de tecnologías digitales. Huella digital: - rastros que dejan los/as usuarios/as al utilizar recursos digitales y su relación con la construcción de la identidad, la ciudadanía.

Criterios de logro

Reflexiona sobre la seguridad de los datos compartidos en internet y redes sociales.
Reconoce aspectos de la construcción de su identidad y huella digital.
Selecciona y utiliza herramientas digitales en producciones colaborativas.
Identifica los riesgos asociados con la publicación de información personal en línea.

Posibles vinculaciones a otros espacios y unidades curriculares.

A definir por maestro/a de aula

Es importante que el contenido puesto en juego durante el proyecto pueda adaptarse a los objetivos de aprendizaje previstos por el DA. Se identifican algunos contenidos del 2do ciclo, que podrían trabajarse:

Matemática:
Introducción a la estadística y a la probabilidad. Gráficos: diagrama de barras, histogramas. Espacio muestral

Lengua Española:
Oralidad. La escucha respetuosa de diversas opiniones y las razones para sostener o modificar las propias. La elección de los temas y la confrontación de ideas. Los argumentos. Las estrategias lingüísticas para la argumentación: palabras para persuadir.
Lectura. Las estrategias discursivas. La construcción de sentido: el vínculo entre párrafos.
Escritura. La práctica de escritura: la selección del tema, la progresión del contenido y la cohesión textual.

Formación de la Ciudadanía:
Diversas formas de habitar los entornos digitales: usuarios consumidores, prosumidores y productores.
La participación democrática en espacios de construcción colectiva.
Ciudadanía digital: Identidad digital Conformación de la Huella digital. Oportunidades y desafíos.

Materiales de referencia
AGESIC. Ciudadanía digital
Derechos de la ciudadanía digital Protección de datos personales
Desafío Bebras de codificación:
https://scratch.mit.edu/projects/603710990

Síntesis de la propuesta

Acuerdos iniciales de coordinación

El diálogo permanente de docentes remotos (DR) y docentes de aula (DA) es fundamental para llevar adelante esta propuesta.

Decisiones del DA → comunicar a DR :

- Las articulaciones con otros contenidos programáticos.

Decisiones DR → comunicar a DA:

- Explicitar al DA semanalmente los objetivos de cada VC y establecer acuerdos en torno a la dinámica de las clases remotas, la organización espacial necesaria y la participación del DA.

Información que necesita tener el DR:

- El proceso de trabajo que realizó el grupo en torno a ciudadanía digital en oportunidades anteriores.
- Experiencias previas en el trabajo con placas micro:bit. tanto de los estudiantes como del DA.

Rol del DA durante las VC

- En las actividades de **inicio** organiza el intercambio para que los estudiantes relaten al DR lo realizado en el aula.
- En las actividades de **desarrollo**, será importante intervenir para vincular el trabajo a lo realizado en el aula y al proyecto global en el que se inscribe esta propuesta.
- En las actividades de **cierre y reflexión**, su participación es fundamental para recuperar momentos que haya observado durante el desarrollo de las actividades y apelar a experiencias previas de los estudiantes que aporten a las reflexiones propuestas por el DR.
- Durante todo el proyecto serán valiosas las acciones del DA que favorezcan el **vínculo** de los estudiantes con el proyecto y el DR.
- Durante los **intercambios**, facilitar la circulación de la palabra, permitirá que todos los estudiantes tengan oportunidad para expresarse.

Rol del DR durante el proyecto

- Anticipar al DA el modo y el contenido planificado para cada VC.
- Indagar los contenidos programáticos que el DA elige para acompañar la propuesta pedagógica y resignificarlos durante la VC.
- Llevar adelante las clases por VC en conjunto con el DA.
- Gestionar el curso en Crea de la propuesta, realizar los ajustes necesarios y las devoluciones a los estudiantes que correspondan.

Recursos y aplicaciones

El DR necesita conocer las experiencias previas por parte de los estudiantes y el DA en el trabajo con placas micro:bit.
En caso de que sea la primera experiencia, en la etapa 1 de la propuesta se presentan dos actividades (Anexo 1) a manera de introducción general al funcionamiento de la placa y su programación. Las mismas implican una breve práctica en:

- El uso del entorno Makecode <makecode.microbit.org>.
- El guardado del programa en un archivo .hex en la computadora.
- La conexión de la placa a la computadora mediante el cable USB.
- El copiado del archivo .hex a la placa a través del administrador de archivos.
- El uso del portador de pilas para que la placa funcione sin cable.

Disponibilidad de placas micro:bit entre los estudiantes
Como mínimo se sugiere tener 1 placa cada 3 o 4 estudiantes e idealmente que la mayoría disponga de su placa. En el sitio https://microbit.ceibal.edu.uy/ sección Recursos y allí Documentos encontrarán respuestas a las preguntas para solicitar una micro:bit.

Tutoriales Micro:bit
En el canal de youtube micro:bit Plan Ceibal, el **video ¿Cómo programar mi micro:bit?** https://youtu.be/pKt5k1wSXSg explica el proceso completo del armado, la programación y la instalación de un programa en la placa *micro:bit*. En el **sitio micro:bit del Plan Ceibal** https://microbit.ceibal.edu.uy/. En la sección "Recursos" está disponible el video Mis primeros pasos o en pdf la Guía básica.

Curso en plataforma Crea ↓

Se destinará una carpeta en Crea para este proyecto dentro del Curso de PC, que contiene una estructura similar a la de esta guía. Este espacio virtual ofrece herramientas de trabajo que servirán al DR a llevar adelante distintos momentos en la VC.

Actividades Interactivas
Las actividades interactivas están pensadas para ser realizadas en distintos momentos en cada etapa. En alguna oportunidad pueden ser una instancia de aprendizaje de los contenidos, en otras pueden formar parte del cierre del desarrollo de la clase. Lo importante es recuperar la resolución de las mismas para realizar una puesta en común.

Foro de evidencias
Los avances del proyecto y las conclusiones abordadas durante el desarrollo del mismo se comparten en los foros de evidencias. Lo importante es que se recupere una o varias evidencias para socializarlas en la VC y enriquecer el intercambio de ideas.

Reflexión y registro de cierre
A lo largo de toda esta propuesta se propone plasmar los intercambios del cierre en **un registro común** para toda la clase que se va enriqueciendo en cada etapa. Cada pareja de docentes considerará la herramienta más adecuada que permita compartir un enlace con los estudiantes en la plataforma. Puede utilizarse un documento compartido para tomar el registro, una página creada en Crea o incluso mapas conceptuales realizados a partir de los intercambios grupales.
Las dinámicas para la escritura en este archivo podrán ir variando entre una etapa y otra. Algunas veces se puede recurrir a la **escritura por parte de los docentes**, otras veces se puede **recopilar respuestas de un foro**, compilar imágenes de **capturas de pantalla** o solicitar **escrituras parciales** a subgrupos.

ETAPA 1 ↓
Mensajes en riesgo

En esta etapa se da inicio al proyecto presentando en el aula los contenidos de ciudadanía digital y en la VC se hacen actividades de comunicación entre placas. El objetivo es poner de manifiesto que al enviar un mensaje en una red de comunicación en la que participan muchas personas es posible que otros destinatarios, además del receptor, lo lean.

En el aula, se enmarca el proyecto en torno a la ciudadanía digital, se organiza la toma de notas para recuperar las nociones sobre circulación de información en Internet trabajadas en el Nivel 1.

En la VC, se experimenta la circulación de información en dispositivos inalámbricos. Se proponen distintos juegos matemáticos en los que una micro:bit envía información a las placas de un grupo y puede ser interceptada por otro grupo.

Objetivos

Se espera que los estudiantes sean capaces de:

- Experimentar el envío, recepción e intercepción de mensajes entre dispositivos a través de medios inalámbricos.
- Reflexionar sobre la vulnerabilidad de los datos enviados en texto plano a través de las redes.

Coordinación dupla pedagógica

Decisiones conjuntas entre DA y DR:

- Repasar el Rol del DA durante la VC a partir de los acuerdos iniciales.
- Conformar grupos de 2 a 4 integrantes para trabajar a lo largo de toda la propuesta..
- Decidir cómo se organizan los equipos para la actividad en la VC (emisores y receptores)

Decisiones del DA

- Formato de la toma de notas grupales.

Información que necesita tener el DR:

- Cómo realizaron la actividad de aula y que dudas surgieron del intercambio.

AULA ↓

Notas para el DA ↓

Derecho a conocer

Propósitos mínimos

- Presentar el proyecto en el marco de la ciudadanía digital.
- Propiciar la resignificación de las características propias de la circulación de información en una red (paso por puntos intermedios, existencia de caminos alternativos).

Propósitos óptimos

- Favorecer la comprensión de que Internet es una red mundial formada por computadoras que intercambian información, a través de juegos y materiales utilizados en otras propuestas de Ciudadanía Digital.

Presentación de la propuesta:
Se presenta el proyecto anticipando a los estudiantes que durante los próximos encuentros abordarán actividades vinculadas a la ciudadanía digital y que para hacer un uso **crítico y responsable** es importante conocer cómo funcionan los dispositivos y cómo se establecen las comunicaciones. Se sugiere compartir con la clase el video Qué es ciudadanía digital

Internet: red de redes
Se propone la realización de una actividad que permita recuperar lo estudiado en el proyecto de nivel 1: "El viaje de la información por Internet". Luego, cada grupo puede dejar registro de esta actividad en el foro en Crea sobre dudas, nuevas preguntas y conclusiones.
Se sugiere utilizar alguna de estas actividades que están disponibles en el aula en Crea. A criterio del DA se puede hacer visible o no.
- Búsqueda Del Tesoro - ¿Por dónde viaja la información que circula por Internet?
- Circulando mensajes - Juego en Scratch sobre recorridos de la información en las redes.

¿Cómo viaja la información en internet? ¿Va de una computadora a otra sin pasar por otros equipos? ¿Por donde viajan los mensajes?

VC ↓
Mensajes en el espacio

💡 Desafío
Resolver los desafíos matemáticos en el menor tiempo posible.

1. Inicio (15 min)
Los estudiantes comparten con el DR las notas y reflexiones que realizaron en el aula con el DA acerca de cómo se comunican los ciudadanos digitales conectados a través de Internet, el cuidado de la privacidad y la protección de los datos personales. El DR anticipa que el objetivo de este proyecto es aproximarnos a comprender cómo funcionan las tecnologías que posibilitan una comunicación segura en nuestra sociedad y destaca la importancia de proteger los datos en una época en la que circulan masivamente.
En aquellos grupos de estudiantes que no tienen ninguna experiencia con las micro:bit, se sugiere que el DR los acompañe en el desarrollo de las actividades propuestas en el Anexo 1 a modo de introducción al entorno, programación y funcionamiento de las placas.

2. Desarrollo (20 min)
Juego de mente con la micro:bit
El DR propone a los estudiantes hacer la experiencia de comunicarse utilizando las placas micro:bit. Para ello presenta un juego en el cual el DA elige un desafío matemático, el DR muestra el enunciado del mismo en la pantalla, los participantes resuelven el cálculo y un asistente verifica qué participante lo resolvió correctamente en menos tiempo. En la experiencia de comunicación, las placas micro:bit se utilizan para enviar y recibir el resultado de los desafíos.
Para poder implementar este juego se necesitan como mínimo tres placas micro:bit, cada una tendrá una función diferente. Por esta razón, en la placa **Emisora** se carga el programa que contiene las respuestas a los desafíos matemáticos, las que se enviarán en primera instancia a la placa **Asistente** y en segunda instancia a las placas **Participantes**.
Con la guía del DR, los estudiantes realizan el siguiente programa en MakeCode y lo cargan en las placas **Participantes** y **Asistente.**

📌 Atención:
En esta instancia, no se espera que los estudiantes descubran cómo programar las micro:bit o que comprendan en su totalidad el código realizado. Pero sí dejar en claro que **cada botón** tiene asociado un **canal de comunicación diferente**: uno **entre el Emisor y el Asistente**, y otro **entre el Emisor y los Participantes**.

1… 2… 3 ¡En marcha!
Antes de realizar la dinámica del juego como se detalla en el Anexo 2, los estudiantes deben presionar el Botón A (Asistente) y Botón B (Participantes) de sus placas para establecer contacto con la radio de la placa Emisora y luego recién, comenzar a jugar. Se espera que los Participantes, a medida que se desarrolla el juego, descubran que pueden captar la respuesta que la placa Emisora envía a la placa Asistente y así interceptar el resultado del cálculo en menos tiempo.

En caso que esto no ocurra, o surja alguna inquietud al respecto, el DR retoma la experiencia y a partir de preguntas cómo:
¿Qué rol cumplen las placas que intervienen en el juego? ¿Para qué necesita la información el asistente del DA y para qué la necesitan los jugadores? ¿Por qué la placa Asistente y las placas Participantes reciben el mensaje en momentos distintos? ¿Qué pasa si un Participante presiona el botón A durante la ronda?,
comparte con los estudiantes que hay un modo de establecer intercambio de información llamado *comunicación por grupos* en el cual, un mensaje es enviado (o recibido) sólo a los dispositivos que forman parte del grupo. Es esta la razón por la cual las placas **Participantes y la Emisora** establecen un canal de comunicación con un número (10) y la placa **Asistente** y la **Emisora** establecen otro canal de comunicación con un número diferente (1). Sin embargo, la experiencia del juego demuestra que el canal de comunicación que se establece entre los grupos es vulnerable, ya que si los participantes descubren qué sucede al apretar el botón A, fácilmente pueden interceptar el mensaje enviado a la placa **Asistente**.

📌 Atención:
Es necesario definir quién maneja la placa Emisora para los juegos, puede ser el DA o un estudiante. El programa para la placa emisora puede enviarse por mensaje privado o como Archivo/Enlace/Herramienta externa en CREA para que quien controle la placa Emisora pueda descargarlo antes de comenzar el juego.

⭐ Importante
Antes del cierre considerar las recomendaciones respecto a la importancia de realizar las **Actividades interactivas**.

3. Cierre (10 min)

¿Cómo es posible que se establezca una comunicación entre las placas? ¿Por dónde viaja esa información? ¿Por qué le llega a todas las placas? ¿Por qué leemos todos el mismo mensaje? Si hay una tercera persona que no conocemos con una placa en la habitación de al lado ¿puede leer nuestro mensaje?
Las placas cuentan con una radio que permite establecer una comunicación entre ellas de manera inalámbrica, es decir, usan ondas de radio para comunicarse. Al contar con la misma tecnología, todas las placas pueden recibir el mismo mensaje de manera simultánea, sólo es necesario que las placas cuenten con la programación adecuada para captar el mensaje y poder verlo. En el caso que un desconocido se encuentre en una habitación cercana (si está en el rango de alcance de las radios), podría interceptar el mensaje y acceder a la información. Esto confirma la vulnerabilidad de datos enviados en texto plano a través de las redes entre dispositivos inalámbricos.
En la vida cotidiana se presentan situaciones en las que enviamos y recibimos información a través de medios inalámbricos. Por ejemplo, cuando utilizamos redes Wi-Fi o transmitimos datos a través de conexiones Bluetooth, estamos interactuando con este tipo de tecnologías que también presentan vulnerabilidades similares a la de las micro:bit.

¿De qué forma viaja la información entre las computadoras y el router Wi Fi? ¿Puede un tercero conectarse y "leer" lo que enviamos y recibimos? ¿Por qué?
La información entre computadoras y el router Wi-Fi también se establece a través de un medio inalámbrico, permitiendo un intercambio de datos a través del aire. Las redes Wi-Fi pueden ser vulnerables y permitir que intrusos intercepten la información y "lean" lo que se envía y recibe. Para evitar esta situación, es necesario proteger la red con medidas de seguridad adecuadas.

Como motivación para la siguiente etapa, puede plantearse:
¿Cómo podemos hacer que alguien que intercepte el mensaje, no pueda comprenderlo? ¿Cómo lo imaginan?

Registro en Crea

El DR publica el registro con las notas y reflexiones de los intercambios en el **Registro Común**.

Invitar a los estudiantes a resolver la actividad interactiva de la etapa.

La Yapa: Propuestas para seguir en casa

Modifica tu programa en la Micro:bit para que pueda enviar mensajes además de recibir.

ETAPA 2 ↓
Mensajes secretos

En esta etapa, se introduce un método de cifrado como respuesta al problema de vulnerabilidad en la transmisión de información, evidenciado en la etapa anterior. Se experimenta con el cifrado César.

En el aula, se realizan una serie de actividades desenchufadas de descifrado y cifrado.

En la VC, se realiza un juego de comunicación inalámbrica con mensajes encriptados en el que solo un equipo posee la clave. A diferencia del juego de la etapa anterior, solo el equipo a quien está destinado el mensaje, puede descifrarlo y comprenderlo.

Objetivos

Se espera que los estudiantes sean capaces de:

- Reconocer el cifrado de mensajes como una herramienta para evitar el acceso de terceros a la información.
- Identificar situaciones en las que es necesario proteger la información.

Coordinación dupla pedagógica

Decisiones conjuntas entre DA y DR:

- Definir qué herramienta usarán con el cifrado César: la plantilla del Anexo 4 (para armar en papel), o el programa en Scratch: Cifrado César.
- Organizar la dinámica de la VC, cómo y quién enviará los mensajes con la Micro:Bit

Decisiones del DA

- Formato de la toma de notas del video y la línea de tiempo.
- Decidir cómo se organizan los equipos para la actividad en la VC (emisores y receptores).

Información que necesita tener el DR:

- Cómo realizaron la actividad de aula y que dudas surgieron del intercambio.

Ceibal | Fundación SADOSKY | <Program.AR/>

AULA ↓
Descifrado y cifrado

Propósitos mínimos

- Proponer actividades para que los estudiantes experimenten y se familiaricen con el cifrado y descifrado de mensajes mediante el código César.

Propósitos óptimos

- Proponer actividades que permitan conocer diferentes tipos de cifrado y sus usos.

Notas para el DA ↓

Cifrado César
Se propone realizar con los estudiantes prácticas de cifrado y descifrado por sustitución, conocido como cifrado César. En el Anexo 3 se presentan algunas actividades posibles.

En el Anexo 4 se facilita una plantilla para recortar y armar que permite descifrar texto de manera manual o pueden utilizar un recurso digital al que acceden a través del siguiente enlace: Cifrado César.

Otros tipos de cifrado
Se deja a disposición de los docentes este recurso educativo abierto de Ceibal a modo de ejemplo que permiten cumplir con los propósitos óptimos: Compresión de texto.

VC ↓
Criptografía

💡 Desafío
Descifrar los mensajes recibidos, con y sin clave, enviados a través de la micro:bit

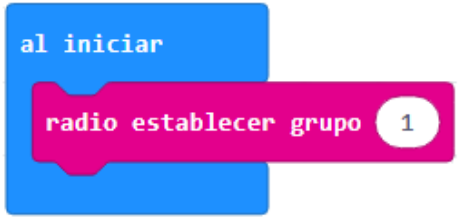
1. Inicio (5 min)

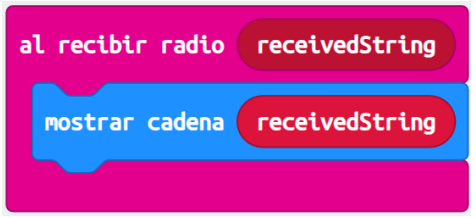
Recordando el Juego de Mente realizado en la VC anterior y las actividades realizadas en el aula, se recupera la experiencia sobre cifrado de mensajes. ¿Cómo podemos hacer para evitar que otra persona intercepte el resultado del cálculo?
El DR retoma el Juego de Mente con la micro:bit realizado en la etapa anterior y la vulnerabilidad que presentaba, ya que otros participantes podían acceder al mensaje de texto plano que se enviaba desde la placa **Emisora**. El cifrado es una alternativa que permite proteger la respuesta en su trayecto al receptor.

📌 Atención:
En caso de no haber realizado la actividad de aula, se recomienda la realización acotada de la actividad 2.1 del Anexo 3 (cifrado César). La misma invita a descifrar la frase "ÑHPWR HV PRUODÑ" con la ayuda de la tabla de Código.

1. Desarrollo (30 min)

Descifrando el mensaje
El DR propone a los estudiantes la realización de una nueva experiencia de comunicación entre placas por radio, pero esta vez, retomando la importancia de que los mensajes enviados estén cifrados, para ello presenta el juego Descifrando el mensaje.
Para implementar este juego se necesitan como mínimo tres placas micro:bit, cada una tendrá una función diferente. Por esta razón, en la **Placa Emisora** se descarga el programa que contiene los mensajes cifrados que enviará a las **Placas Receptoras** y; con la guía del DR, los estudiantes realizan el siguiente programa en MakeCode para luego descargarlo en las **Placas Receptoras.**





1… 2… 3 ¡A descifrar!
En el Anexo 5 se detalla la dinámica del juego propuesto. A medida que se desarrolla la misma, los estudiantes experimentan y analizan en qué situación les resulta más rápido descubrir el mensaje. A la conclusión que se espera que arriben es que con la clave (cantidad de corrimiento de lugares en el abecedario), es más rápido descifrar el mensaje.
Luego de finalizadas las dos rondas, el DR retoma la experiencia y orienta la reflexión del juego:
¿Quiénes pudieron descifrar cada mensaje? ¿Los receptores que tenían la clave lograron descifrar el mensaje más rápido? ¿Por qué?
Se guían las reflexiones a valorar el cifrado de los mensajes, ya que al disponer de la clave resulta más sencillo descifrarlos, caso contrario, la

seguridad del cifrado y la complejidad de probar diversas claves complica la tarea de comprender el mensaje.

> ⭐ Importante
> Antes del cierre considerar las recomendaciones respecto a la importancia de realizar las **Actividades interactivas**.

3. Cierre (10 min)

¿Cómo harían para que sólo algunos entiendan el mensaje que enviaron? ¿Por qué creen que es importante cifrar los mensajes que envían con las placas?

Cifrar los mensajes que se envían de una placa a otra, ayuda a garantizar la seguridad y privacidad de la información, disminuyendo el riesgo que un receptor que no deseamos comprenda el contenido del mensaje. El DR comenta, que la información viaja codificada entre los dispositivos y esa codificación forma parte de lo que se llama encriptación. Una práctica que la humanidad lleva siglos desarrollando para ocultar información en sus comunicaciones. Se les sugiere a los estudiantes observar el video de la yapa para profundizar en el tema.

¿En qué situaciones de la vida cotidiana les parece necesario que la información esté encriptada? ¿Por qué? ¿Qué ejemplos se les ocurren? ¿Qué pasaría si no existiera el encriptado en Internet?

Es necesario que la información esté encriptada en situaciones en las que se manejan datos sensibles o confidenciales, por ejemplo: envío de correo electrónico, compras en línea y transacciones bancarias, intercambio de información confidencial por mensajería instantánea, etc. En estos casos la encriptación asegura la su confidencialidad, asegura que los datos estén protegidos durante la transmisión del mensaje entre el emisor y receptor.

Registro en Crea

El DR publica el registro con las notas y reflexiones de los intercambios en el **Registro Común**.

Invitar a los estudiantes a resolver la actividad interactiva de la etapa.

La Yapa: Propuestas para seguir en casa

Si quieres saber más sobre la Criptografía en nuestra vida cotidiana puedes ver este video

Los Códigos Secretos de la Historia - Los Creadores

ETAPA 3 ↓
Cierre

El objetivo de esta etapa es poner de manifiesto que las computadoras son herramientas que facilitan el proceso de cifrado y descifrado de información.

En el aula, se realiza un análisis de caso sobre vulneración de la información producto de un error humano.

En la VC, se descifran mensajes sin conocer la clave de cifrado, primero manualmente y luego con la ayuda de la computadora.

Objetivos

Se espera que los estudiantes sean capaces de:

- Reconocer que es posible descifrar un mensaje aún si se desconoce la clave de cifrado.
- Identificar la utilidad de las computadoras para descifrar mensajes.
- Relativizar la seguridad de la información, por el método de cifrado elegido y por las acciones de las personas que la utilizan.

Coordinación dupla pedagógica

Decisiones conjuntas entre DA y DR:

- Cómo realizar el cierre del proyecto, este puede ser un buen momento para organizar una publicación de notas sobre lo aprendido.

Decisiones del DA

- Cómo abordar el análisis de caso sugerido.

Información que necesita tener el DR:

- Cómo realizaron la actividad de aula y las reflexiones del caso analizado.

AULA ↓
Gestión de la información

Propósitos mínimos

- Propiciar un espacio para el análisis del caso de la página 24 de Guía didáctica de seguridad de la información para poner de manifiesto la responsabilidad humana en la seguridad de la información.

Propósitos óptimos

- Acompañar a los estudiantes en la organización de una campaña escolar de sensibilización sobre la seguridad de la información en internet.

Notas para el DA ↓

Un caso de inseguridad informática: El profesor de historia
Se sugiere realizar la actividad Casos para analizar y reflexionar Caso 1: Profesor de Historia de la Guía didáctica de seguridad de la información, reproducida en el Anexo 6.
¿Qué situación es la que generó el caso de inseguridad? ¿Cuáles pueden ser las consecuencias de este fallo en la seguridad?

Campaña de sensibilización sobre seguridad informática
El DA define el modo de llevar adelante la campaña de sensibilización sobre seguridad de la información en internet, en conjunto con los estudiantes. Es posible trabajar con afiches, podcast, presentaciones, videos, juegos, etc. Se sugiere compartir esta producción con el resto de la comunidad educativa y la familia.

VC ↓
Descifrando con computadoras

💡 Desafío
Descifrar mensajes sin conocer la clave.

1. Inicio (5 min)
¿En qué consistía el caso del profesor de historia? ¿Por qué la información en su computadora resultó vulnerable?

El DR realiza una puesta en común del caso del profesor con el objetivo de analizar la vulnerabilidad de la seguridad de la información relacionada a las acciones que realizan las personas. Cifrar los datos no es garantía de seguridad si se deja al alcance de terceros las claves o los datos descifrados. El cifrado es una solución técnica, pero debe ir acompañada de acciones de los usuarios que no vulneren la seguridad de la información.

📌 Atención:
En caso de que en la clase de aula no se haya podido introducir el Caso 1: Profesor de Historia (Anexo 6), se recomienda introducirlo brevemente al inicio de la VC.

2. Desarrollo (30 min)
El DR propone a los estudiantes participar de un juego para descifrar mensajes, primero sin computadora, y luego con ella. El objetivo de este juego es descifrar los mensajes que el DR muestra en su pantalla compartida.

📌 Sugerencia:
Para motivar a los estudiantes y generar una dinámica de juego, el DR puede utilizar un cronómetro digital en su pantalla compartida para controlar el tiempo en que tardan en descifrar los mensajes.

En un primer momento, los docentes comparten con los estudiantes un mensaje cifrado: CFKXKOCOBC y les propone descubrirlo utilizando la plantilla disponible en el anexo 4 (cifrado César). Tener en cuenta que **no se les debe dar la clave**. El DR ofrece un tiempo para que prueben distintas posibilidades de descifrado hasta descubrir el mensaje y compartir los resultados del proceso realizado. Al realizar un corrimiento hacia la izquierda de 2 caracteres obtienen la palabra ADIVINANZA.

📌 Atención:
El DR puede utilizar un corrimiento de caracteres mayor si el grupo de estudiantes tiene práctica con el uso del cifrado César.

En un segundo momento, los docentes presentan a los estudiantes otro mensaje cifrado: WCZMUXJ WYNUM y les propone descubrirlo utilizando una nueva herramienta: Calculadora en línea: Cifrado César para descifrar el mensaje.
El DR ofrece un tiempo para que prueben la herramienta y descubran entre las opciones que ofrece la computadora, cuál es el mensaje descifrado. Se espera que obtengan el mensaje descifrado: CIFRADO CÉSAR.

Analizando las dos experiencias realizadas en el juego, *¿qué mensaje descifraron más rápido? ¿Por qué? Al utilizar la computadora para descubrir el segundo mensaje, ¿les hubiera facilitado la tarea conocer la clave? ¿Por qué?*

Se realiza una puesta en común sobre la experiencia y el DR pone de manifiesto que si bien la plantilla de cifrado César les permitió

descifrar el mensaje de manera manual en la primera experiencia, utilizando la computadora, con el mismo método de cifrado, lograron descubrir el mensaje en menos tiempo y sin errores. En ambos casos desconocían la clave, pero para el descifrado manual hubiera sido un facilitador, en cambio para el descifrado con la computadora no es tan necesario la misma ya que es capaz de procesar los 26 corrimientos posibles rápidamente.

📌 Sugerencia:
En caso que el DR considere apropiado presentar otros mensajes, considerar que para el descifrado manual es recomendable elegir una clave baja y para el descifrado en computadora, una clave alta, con la intención de dejar en evidencia las ventajas y desventajas en cada caso.

⭐ Importante
Antes del cierre considerar las recomendaciones respecto a la importancia de realizar las **Actividades interactivas**.

3. Cierre (10 min)

¿Es posible descifrar un mensaje sin conocer la clave? ¿Con cuál de las experiencias realizadas en la VC lo lograron? ¿Por qué es tan valioso el rol de la computadora para descifrar mensajes?

El DR habilita un espacio de reflexión sobre las ventajas que ofrecen las computadoras en los procesos de cifrado y descifrado sin clave. En la experiencia realizada, si bien descubrieron la palabra probando distintos corrimientos de forma manual, les llevó mucho tiempo. Si en lugar de una palabra, el texto a descifrar hubiera sido más extenso, el proceso habría llevado más tiempo aún. Sin embargo, comprobamos que, la capacidad de procesamiento de una computadora, permite descifrar un mensaje extenso, con una clave desconocida, de manera eficiente y en menos tiempo.

¿Servirá el cifrado César para enviar datos por la red? ¿Conocen otros tipos de cifrados y dónde se usan? Aunque los mensajes que enviamos están encriptados y es difícil que alguien que los intercepte pueda leerlos, ¿qué acciones del usuario pueden perjudicar la confidencialidad de sus datos?

El DR realiza una puesta en común para reflexionar acerca de la vulnerabilidad del cifrado César, ya comprobado en la experiencia del aula. De manera manual o utilizando la computadora logramos descifrar los mensajes.

El DR comparte con los estudiantes la existencia de distintos métodos que se utilizan actualmente en tecnologías digitales. Si bien son más complejos de cifrar, son tan difíciles de descifrar que, aún utilizando computadoras, no es factible encontrar la clave en un tiempo razonable. Por ejemplo: gpg, llave pública y privada, encriptado asimétrico, certificados, vpn entre otros. Los métodos de cifrado de datos se utilizan en distintas aplicaciones: mensajería instantánea, correo electrónico, redes sociales, transferencias bancarias, entre otros.

En el ejemplo visto en clase, el docente de historia podría haber tomado medidas adicionales para proteger la información confidencial que guardaba en su dispositivo, por ejemplo, haber creado una contraseña de acceso, bloquear su pantalla si por determinado tiempo no la usaba, cerrar sesión en caso de estar utilizando una computadora compartida con otros, hubiera evitado el acceso de terceros a su información. Estas acciones son importantes si consideramos que el cifrado es una solución técnica, pero debe ir acompañada de acciones de los usuarios que no vulneren la seguridad de la información.

Registro en Crea

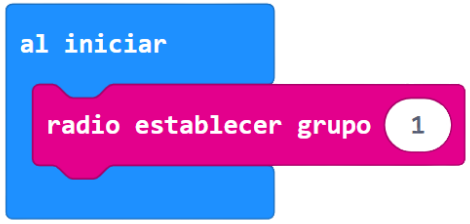
El DR publica el registro con las notas y reflexiones de los intercambios en el **Registro Común**. Se lleva a cabo la socialización organizada previamente con el DA.

📑 ANEXO 1

¡A programar la placa micro:bit!: ¿cómo recibir y enviar mensajes?

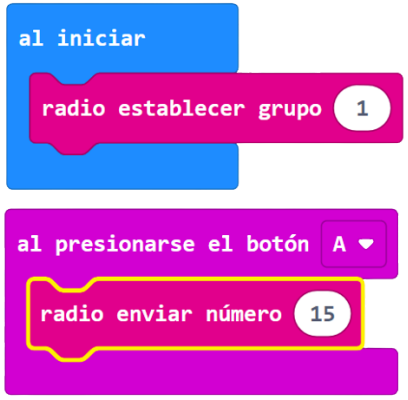
El DR propone a los estudiantes hacer la experiencia de **comunicarse** utilizando las placas micro:bit. Esto es posible porque cuentan con una **radio** incorporada en las placas que permite enviar y recibir todo tipo de datos digitales. La comunicación que propone se llama **comunicación por grupos,** es decir que el mensaje es enviado desde una placa a otras solo si pertenecen a un mismo grupo.
Una opción para organizar la experiencia es que los estudiantes se dividan en grupos con varias micro:bit a programar. El DR los guiará utilizando la plataforma MakeCode.

Paso 1: Creación de grupos para comunicarse por radio
Cada grupo elige un número único entre 0 y 255, luego configuran las radios de las placas con ese número. Para ello deben usar el bloque "radio establecer grupo".



¿Qué pasaría si dos grupos eligen el mismo número?¿Cómo asegurarnos de que esto no ocurra? Se sugiere que la DA registre el número elegido por cada grupo y confirme que no hay grupos con números repetidos.

Paso 2: Envío y recepción de mensajes
Una vez creado el canal de comunicación por grupo, el DR propone crear un programa que permita a una placa, enviar un dato a las demás placas del grupo y los acompaña en la realización del mismo.
Cada estudiante emisor del mensaje programa su micro:bit para enviar, por ejemplo, un **número** cualquiera a su grupo al presionar un botón. Para ello deben usar el bloque de entrada "al presionar el botón" y "radio enviar número".



Luego, el DR muestra cómo es el procedimiento por el cual se descarga el programa creado en Makecode a la placa emisora del mensaje.

¿Qué faltaría programar para que los demás estudiantes reciban y vean en sus placas el número enviado?
Cada estudiante receptor del mensaje programa, orientado por el DR, su micro:bit para recibir y ver por un tiempo el número enviado por el emisor. Para ello deben usar el bloque de entrada "al recibir radio" y "mostrar número recibido".

Al finalizar, el DR muestra el procedimiento de descarga del programa realizado en Makecode en las placas receptoras del mensaje.

Una vez que cada estudiante tiene descargado el programa correspondiente en su placa, lo prueban y sacan conclusiones respecto a su funcionamiento.
¿Quiénes participaron en el intercambio de información en el grupo? ¿Qué rol cumplió cada uno? ¿Cómo hicieron para que una placa envíe el mensaje y otras lo reciban? Además de enviar un número, ¿qué otro tipo de mensajes podrían enviar y recibir? ¿Cómo lo harían?
El DR dedica el tiempo que considere necesario en realizar distintas experiencias de envíos (íconos, texto, esperas entre un mensaje y otro, etc) con el propósito de familiarizarse y agilizar la operatoria de programar envío y recepción de mensajes y la descarga y prueba del programa correspondiente a las placas micro:bit.

Volver Etapa 1

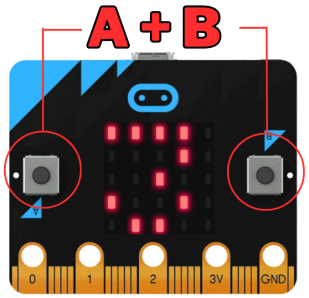
ANEXO 2
Juego de mente con la micro:bit

Objetivo: Resolver desafíos matemáticos en el menor tiempo posible.

Recursos: Placa Emisora con programa cargado, Placa Asistente y Placas Participantes (se programan en la VC).

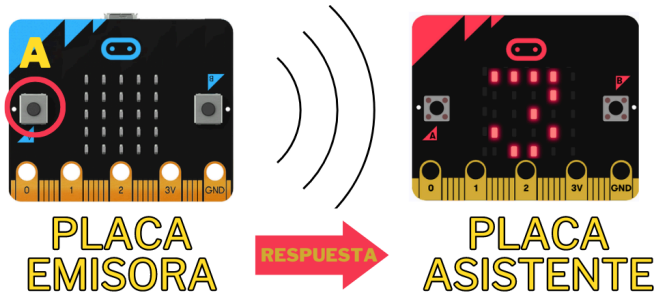
Participantes: Emisor del mensaje con su placa micro:bit, Asistente con su placa micro:bit, y los Participantes que pueden tener una placa por cada uno o una placa por equipo dependiendo de la cantidad de placas disponibles.

Dinámica: Para comenzar el juego, el DA o quien elija como Emisor del mensaje, elige un desafío matemático de los cinco disponibles, lo hace presionando las teclas A+B desde su placa Emisora hasta llegar al número del desafío elegido. Por ejemplo, al número 1. Una vez elegido se lo comunica al DR.



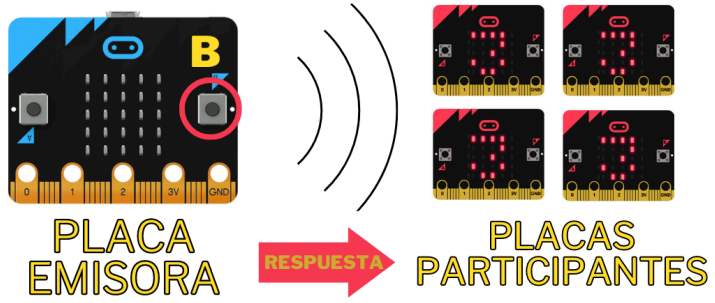
Una vez seleccionado el desafío, el DR muestra en pantalla la tarjeta correspondiente al desafío elegido. En este ejemplo el número 3.

Mientras los Participantes resuelven el desafío matemático, el DA presionando el botón A desde su placa Emisora, envía la respuesta a la placa del Asistente.



Los Participantes intentarán resolver en el menor tiempo posible el desafío comunicando la respuesta de forma oral al Asistente, el primero que lo haga ganará la ronda.

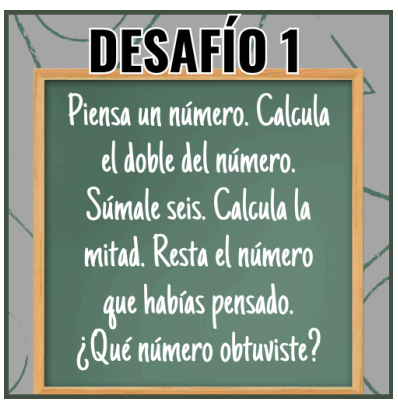
Una vez finalizada la primera ronda, el DA envía la respuesta a las placas Participantes presionando el botón B, esto permitirá que los jugadores puedan verificar si el resultado obtenido es correcto o incorrecto. De este modo se da por terminada la primera ronda, el ganador obtiene un punto y se da comienzo a la próxima ronda repitiendo la misma dinámica.

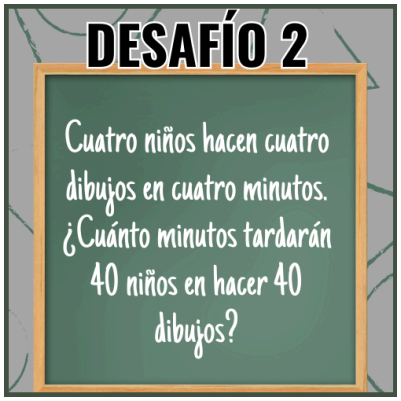


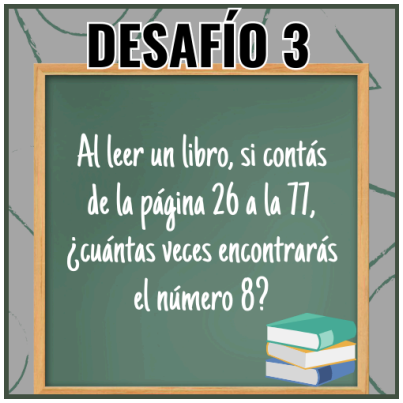
Ganador: Gana el estudiante o equipo que comunique al Asistente primero, la respuesta correcta.

Ceibal | Fundación ADOSKY | <Program.AR/>

Desafíos Matemáticos:







Respuestas:

Desafío 1: **3**
Desafío 2: **4**
Desafío 3: **5**
Desafío 4: **8**
Desafío 5: **8**

Volver Etapa 1

📑 ANEXO 3
Actividad desenchufada.

Actividad 1: Bebras Código Secreto

1. Descifrar el mensaje del castor:
El castor quiere enviar un mensaje secreto a su amiga la liebre. Ellos crearon un código secreto para encriptar el mensaje. Así nadie puede leerlo. En su código secreto, los signos de puntuación no cambian. Las letras son reemplazadas por **la siguiente** letra del abecedario y la Z, se cambia por la A.
¿Cómo escribiría el castor “HACEME UNA LLAMADA” usando este código secreto?
A: IAFEOE PA ÑÑAOAFA
B: TAYEUE UÑA IIAUAEA
C: JAVEQE UZA QQAMARA
D: IBDFNF VÑB MMBNBEB

Actividad 2: Mensajes cifrados

1. Descifrar un mensaje:
Descifrar el siguiente mensaje teniendo en cuenta que el mensaje original se cifró con un corrimiento de 3 lugares. Por ejemplo: la letra Ñ del mensaje cifrado corresponde a la letra L del mensaje original. Para completar la tarea, pueden ayudarse con la tabla de Código.

Mensaje Cifrado	ÑHPWR HV PRUODÑ
Mensaje descifrado	L _ _ _ _ _ _ _ _ _ _ _ _ _ _

Abecedario con clave 3																								
D	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**Ñ**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	**A**	**B**	**C**
Abecedario:																								
A	B	C	D	E	F	G	H	I	J	K	**L**	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z

2. Envíale un mensaje cifrado a otro equipo.
Para escribir un mensaje cifrado, pueden ayudarse usando la tabla de código que muestra un **corrimiento de 3** lugares en el abecedario. Si utilizan la rueda de cifrado César en Scratch o en formato papel, pueden asignarle otro corrimiento.

3. Descifra el mensaje que te envía un equipo.

Respuestas:

Actividad 1: Bebras Código Secreto

Respuesta: D

Actividad 2: Mensajes cifrados

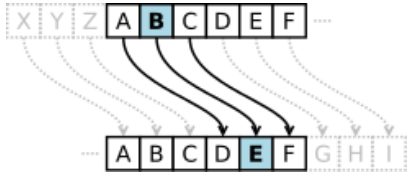
Respuesta: LENTO ES NORMAL

Volver Etapa 2

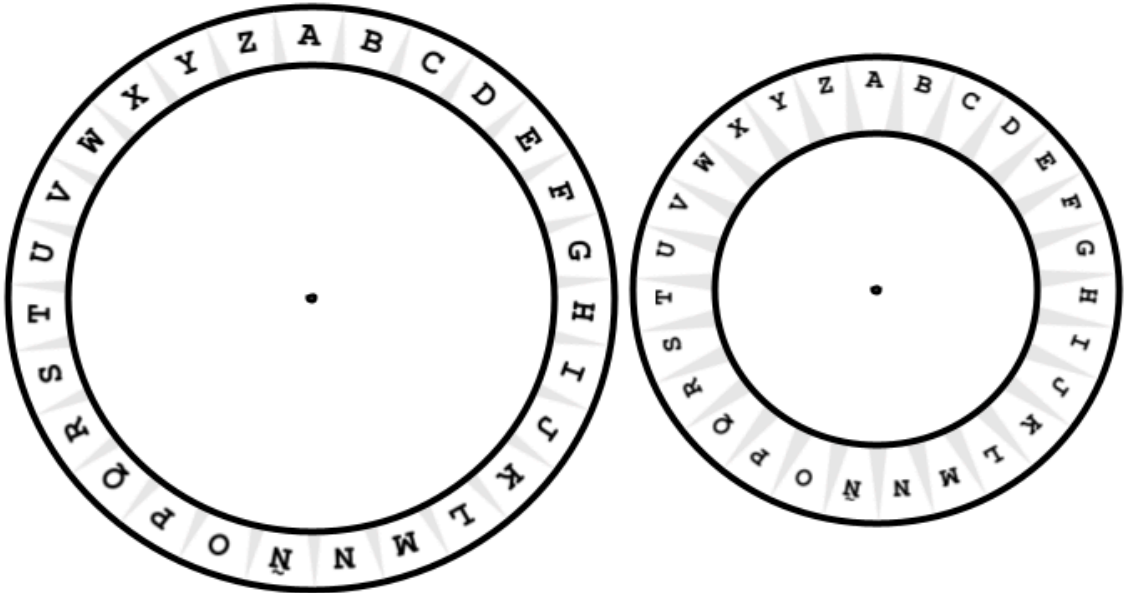
ANEXO 4

Descifrando código

En criptografía, el cifrado por sustitución es un método de cifrado por el que unidades de texto plano (cada carácter) son sustituidas con texto cifrado siguiendo un sistema regular; es decir, cada carácter es cambiado por otro siguiendo un patrón.
Uno de los cifrados por sustitución más famoso es el cifrado César



Podés usar estas plantilla para armar tu cifrado César



Volver Etapa 2

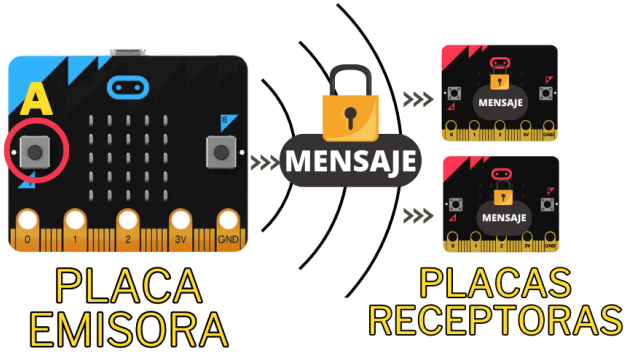
📑 ANEXO 5
Descifrando mensajes

Objetivo: Descifrar los mensajes que las micro:bit reciben.

Recursos: Placa Emisora con programa cargado, Placas Receptoras (se programan en la VC).

Participantes: Un Emisor del mensaje con su placa micro:bit y dos equipos Receptores con su correspondientes placas . Los receptores pueden tener una placa por cada uno o una placa por equipo dependiendo de la cantidad de placas disponibles.

Dinámica: Para comenzar el juego, el DA o quien elija como Emisor del mensaje, presiona un botón desde su Placa Emisora (en la primera ronda el botón A y en la segunda el B). Dicha acción, enviará un mensaje cifrado a las Placas Receptoras.



Las Placas Receptoras de ambos equipos recibirán el mensaje cifrado y los estudiantes intentarán descifrarlo. Mientras tanto, el DA facilitará **sólo a uno** de los equipos la clave para descifrar el mensaje.

Por ejemplo, en la primera ronda, el DA le da la clave de descifrado 4 al equipo A y en la segunda ronda le dará la clave 6 al equipo B.

En la primera ronda, con clave 4, el mensaje descifrado es: HOLAMUNDO

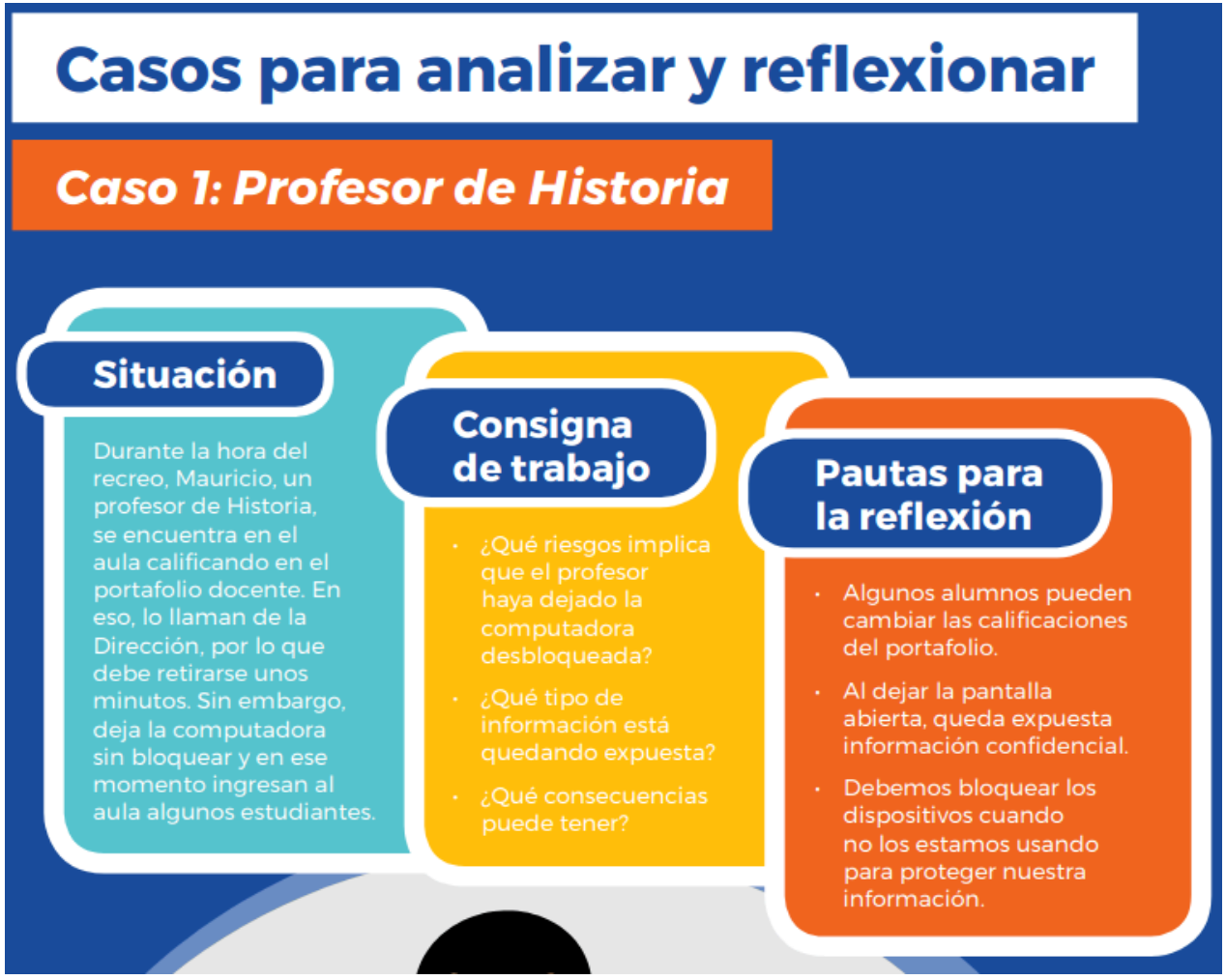
En la segunda ronda, con clave 6, el mensaje cifrado es: BUENDIA

El grupo que primero que primero logre descifrar el mensaje, lo anuncia a la clase, dando por finalizada la ronda con un ganador.

Ganador: Gana el estudiante o equipo que descifre primero el mensaje.

Volver Etapa 2

📑 ANEXO 6
Gestión de la información



Fuente: Guía Didáctica de Seguridad de la Información, ANEP-AGESIC (p. 24)

Volver Etapa 3

Ceibal | Fundación ADOSKY | <Program.AR/>