Cripto:bit

Criptografía en la vida cotidiana

La construcción de la ciudadanía es un proceso de múltiples facetas que se entraman en las acciones cotidianas y en el conocimiento de los elementos que, como partícipes de la sociedad, se ponen en juego al interactuar con nuestros pares. Un ciudadano pleno tiene derecho a conocer cómo funcionan y por qué se utilizan determinadas tecnologías que impactan día a día en nuestra vida cotidiana.

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 ●Eventos

Competencias Marco Curricular Nacional

Dominio PENSAMIENTO Y COMUNICACIÓN.

Competencias: en comunicación, en pensamiento computacional y pensamiento crítico.

Dominio RELACIONAMIENTO Y ACCIÓN.

Competencias: en ciudadanía local, global y digital.

Perspectiva de género

La propuesta de PC busca propiciar una experiencia educativa inclusiva y promotora de equidad de género. No existe una competencia informática inherente a un género en particular sino una desigualdad en el acceso y las posibilidades de varones y mujeres. Para superar esta desigualdad, buscamos:

- incentivar especialmente el trabajo de las niñas y brindarles todas las herramientas necesarias (atención, apoyo, retroalimentación positiva, entre otras),
- desnaturalizar en forma constante el sesgo de la computación y la programación como tarea exclusiva de varones.

Posibles vinculaciones con el Programa de Educación Inicial y Primaria

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:

Área de Conocimiento Matemático.

- La producción de información estadística.
- Los datos estadísticos: El análisis de la frecuencia de los sucesos. La representación en tablas.
- La información estadística: La descripción e interpretación de la información en tablas. La representación gráfica de la información. El uso de la planilla de cálculo en la información estadística.

Área de Conocimiento de Lengua:

- El trabajo con un texto narrativo
- El debate a través de la exposición de opiniones. Argumentos y contra- argumentos.
- Lectura inferencial: el mensaje global del texto. Relacionar información utilizando inferencias textuales y lógicas.
- Producción de textos adecuados a la situación de enunciación.

Área de Conocimiento Social-Ciudadanía

-Uso responsable y seguro de internet. Cuidado de datos personales.

-Uso crítico y reflexivo de internet. Análisis de datos para la toma de decisiones.

Materiales de referencia

AGESIC. Ciudadanía digital ● Derechos de la ciudadanía digital ● Protección de datos personales ● Guía didáctica de seguridad de la información ●

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 conjuntas DA-DR:

- Las aplicaciones y formatos que se pondrán a disposición para el informe digital a realizarse durante el proyecto(Canvas, Scratch, Wordle, Video minuto, documento colaborativo, etc).
- Definir forma de registro de actividades de reflexión.

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.
- 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 del DA, el DR realiza una introducción sobre el funcionamiento de la placa, especialmente destinada a anticipar la dinámica de trabajo y la operatoria de las placas que sucederá en todas las VC de la propuesta:

- 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.

Seguramente se irá afianzando este procedimiento en forma paulatina a partir de la colaboración entre DA y DR.

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. Cada subcarpeta corresponde a una etapa prevista que el DR hará visible a medida que sea necesario.

Este espacio virtual funciona como guía de referencia durante todo el recorrido propuesto. Además de las consignas de trabajo, se encuentran los foros de intercambio, tareas y actividades interactivas.

Los estudiantes publicarán allí tanto los enlaces o avances en sus notas como los informes.

Registro ↓

A lo largo de toda esta propuesta se propone plasmar los intercambios producto de las actividades de cierre en **un registro común para cada grupo de estudiantes** que se va enriqueciendo en cada etapa en la forma de **Notas Grupales.** 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 realización de una **recapitulación general** para que los grupos tomen notas, otras veces se puede **recopilar respuestas de un foro**, compilar imágenes de **capturas de pantalla** o solicitar **escrituras parciales** a subgrupos.

ETAPA 1 ↓
Criptografía y privacidad

En esta etapa se da inicio al proyecto a través de la presentación en el aula de los contenidos de ciudadanía digital y se hacen actividades de comunicación entre placas en la VC. El objetivo es poner de manifiesto que al enviar un mensaje en una red de comunicación en la que participa mucha gente 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 el registro del proyecto y se recupera 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. Mediante un juego de adivinanzas, se simula el envío de información que es interceptada por un 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 ↓
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

Notas para el DA ↓

Se sugiere presentar el proyecto anticipando a los estudiantes que durante los próximos encuentros abordarán actividades vinculadas a la ciudadanía digital, para hacer un uso **crítico y responsable** es importante conocer cómo funcionan los dispositivos y comunicaciones. Se sugiere compartir con la clase el video Qué es ciudadanía digital

Se propone que cada grupo elabore un "cuaderno de notas" en el cual puedan escribir sus dudas, preguntas y conclusiones. Para empezar la escritura en este registro se propone realizar una actividad para reponer y registrar lo estudiado en el proyecto de nivel 1: El viaje de la información por Internet
¿Cómo viaja la información en internet? ¿Va de una computadora a otra sin pasar por otros equipos? ¿Por donde viajan los mensajes?
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.

VC ↓
Mensajes en el espacio

💡 Desafío
Descubrir los números enviando y recibiendo mensajes con la micro:bit.

1. Inicio (15 min)
Los estudiantes, con la guía de la DA, comparten con el DR la actividad que realizaron en el aula.
El DR abre una espacio de diálogo para retomar las notas sobre lo que saben acerca de la criptografía. Anticipa que el objetivo de este proyecto es dar cuenta de algunos elementos de este tema. El objetivo de este breve intercambio es recuperar el tema de estudio del proyecto para enmarcar las actividades de la clase.

2. Desarrollo (20 min)
Utilizando el módulo de radio de las micro:bit se organiza un juego que tiene tres iteraciones o tandas. El DR comenta cómo se organizará el juego y se asignan los grupos.

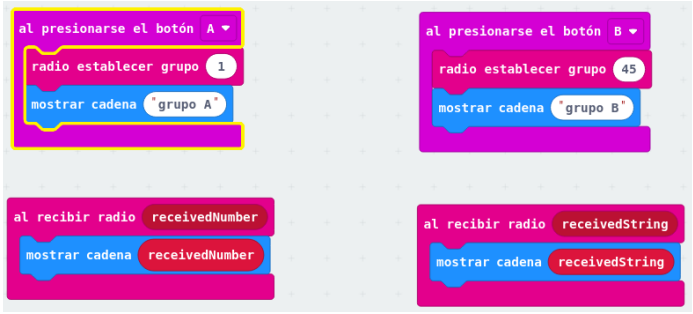
Adivinanzas con la Micro:Bit.
El objetivo de este juego es resolver las adivinanzas de los docentes y verificar las soluciones con la Micro:Bit.
Hay tres equipos **un equipo emisor y dos equipos receptores** simulan ser computadoras, el equipo emisor sólo puede emitir las instrucciones del juego, la adivinanza y responder a una sola pregunta de cada equipo con SÍ o NO.

📌 Atención:
Se define un equipo emisor que puede ser un grupo de estudiantes o el DA. Esta decisión tiene que tomarse en función del manejo de las Micro:Bit que tenga el grupo y la DA. El programa del equipo emisor puede enviarse por mensaje privado o como Archivo/Enlace/Herramienta externa en CREA para asignarla a un estudiante en particular. De modo alternativo, se puede cargar la microbit utilizando la computadora de la DA que podrá ver las páginas no publicadas donde se encuentran los programas.

Los equipos receptores pueden: consultar las instrucciones o la adivinanza las veces que quieran, hacer una pregunta que se pueda responder con SÍ o NO y arriesgar una respuesta por tanda.

Iteración 1: Adivinamos un número y verificamos la respuesta

1. **Carga del programa de adivinanza por el grupo emisor:** Quien oficie de emisor carga el programa adivinar-el-numero-1.hex en su placa.
2. **Instrucciones de carga:** El DR solicita a los estudiantes receptores que realicen el siguiente programa para que las placas puedan escuchar en dos canales:



3. **Instrucciones de uso:** El DR comenta que cada grupo tiene un canal de radio distinto. Para seleccionar el canal de radio, cada grupo tiene que tocar el botón correspondiente a la letra de su grupo. El grupo A toca el botón A y el grupo B toca el botón B. Los estudiantes confirman la selección del grupo leyendo el mensaje de la Micro:Bit.
4. **Adivinanza:** ¿Cuál es el primer número de dos cifras, múltiplo de 2, de 3 y de 4?
5. **Ronda de respuestas:** Cada grupo tiene una oportunidad para hacer una pregunta y una oportunidad para dar una respuesta.
6. **Verificación:** Los docentes avisan que van a emitir un mensaje a las placas para verificar la respuesta. Se emite el mensaje a cada grupo.

Iteración 2: Adivinamos un número y un equipo verifica la respuesta
Esta vez, uno de los equipos, junto a la DA, simulará ser la computadora

1. **Instrucciones de carga:** Quien oficie de emisor carga el programa adivinar-el-numero-2.hex en su placa.
2. **Instrucciones de uso:** Mismas que Iteración 1
3. **Adivinanza:** Es un número que está entre 2000 y 3000 y tiene todas sus cifras iguales.
4. **Ronda de respuestas:** El grupo que responde tiene una oportunidad para hacer una pregunta y una oportunidad para dar una respuesta.
5. **Verificación:** El grupo emisor avisa que van a emitir un mensaje a las placas para verificar la respuesta. Se emite el mensaje a cada grupo.

Iteración 3: Escuchamos las respuestas, pensamos las adivinanzas
Esta vez, **un** grupo va a estar recibiendo la respuesta. Ese grupo no puede decir nada ni ayudar al grupo que responde. El DR advierte al equipo que responde por qué canal emitirá la respuesta a la computadora (A o B). El objetivo es que el equipo que responda intercepte la respuesta e invente una adivinanza para ese número.

1. **Instrucciones de carga:** Quien oficie de emisor carga el programa adivinar-el-numero-3.hex en su placa
2. **Instrucciones de uso:** Mismas que Iteración 1
3. **Adivinanza:** debe ser creada por el grupo que recibe el número del emisor. Por ejemplo para el número 12: Es un múltiplo de 6. Por lo tanto, también de 2 y de 3, es más pequeño que el resultado de 168:12 y más grande que una decena.
4. **Ronda de respuestas:** El grupo que responde tiene una oportunidad para hacer una pregunta y una oportunidad para dar una respuesta.

Ejemplo para la dinámica

- *Emisor*: envía un número.
- *Grupo A*: Recibe el número del emisor e inventa la adivinanza.
- *Grupo B*: Adivina, **pero** el propósito es que descubran que pueden captar la respuesta simplemente presionando el botón del grupo A.

3. Cierre (10 min)

Se realiza una puesta en común a fin de:
- Reflexionar en torno a cómo viaja y se distribuye la información entre dispositivos inalámbricos.
¿Cómo llega la información a 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?
- Reflexionar en torno a qué vulnerabilidades presenta el envío de información entre dispositivos y reconocer situaciones de la vida cotidiana en las que hay envío de información inalámbrica.

¿La información entre las computadoras y el router wifi viaja de la misma forma? ¿Puede un tercero conectarse y "leer" lo que enviamos y recibimos? ¿Por qué?

Como motivación para la siguiente etapa, puede plantearse:
¿Podemos hacer que no todos puedan leer lo que envío, sino sólo quienes decidimos los emisores?

Registro en Crea

Registro en las notas grupales de las conclusiones.
Publicación de notas grupales.

La Yapa: Propuestas para seguir en casa

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

ETAPA 2 ↓
Códigos secretos

En esta etapa, se introduce un método de cifrado como respuesta al problema, evidenciado en la etapa anterior, que en una red no solo el destinatario de un mensaje es capaz de recibirlo y leerlo. Se experimenta con el cifrado César.

En el aula, se realiza 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. Entonces, a diferencia del juego de la etapa anterior, solo el equipo a quien está destinado puede descifrar y comprender el mensaje.

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:

- 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.

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.
- Brindar un espacio para construir ambas ruedas de cifrado.

Propósitos óptimos

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

Notas para el DA ↓

Se sugiere realizar con los estudiantes una serie de actividades de cifrado y descifrado por sustitución (cifrado César).

- Actividad desenchufada: Descifrando un código

Se deja a disposición de los docentes este recurso educativo abierto de Ceibal a modo de ejemplo para cumplir con los propósitos óptimos: https://rea.ceibal.edu.uy/elp/compresion-de-texto/index.html

VC ↓
Criptografía

💡 Desafío

Descifrar los mensajes recibidos con y sin clave enviado a través de la micro:bit

1. Inicio (5 min)

El DR realiza una puesta en común con el objetivo de analizar la actividad del aula. *¿Cómo harían para evitar que un tercero pueda leer sus mensajes? ¿Conocían el cifrado César? ¿Les pareció complicado? ¿Conocen otros métodos de cifrado?*

> 📌 Atención:
> En caso de que no se haya podido realizar la actividad de aula, se recomienda la realización acotada de un desafío de cifrado César. Por ejemplo, se sugiere tomar la frase "ÑHPWR HV PRUODÑ" y la tabla del anexo 2.

1. Desarrollo (30 min)

Utilizando el módulo de radio de las micro:bit se organiza un juego que tiene dos iteraciones o tandas. El DR comenta cómo se organizará el juego y se asignan los grupos.

Descifrando códigos

El objetivo de este juego es descifrar los mensajes que las Micro:Bit reciben.

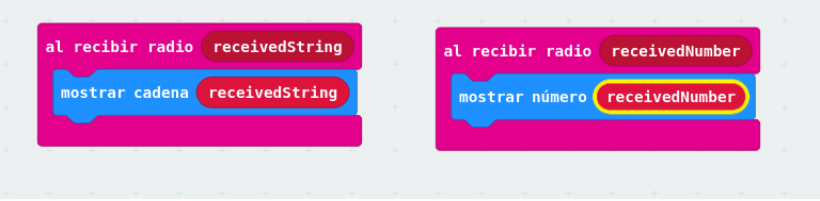
Hay tres equipos: **un equipo emisor y dos equipos receptores**. Se sugiere enmarcar la actividad en una situación narrativa en la cual los equipos receptores están "escuchando" el envío de mensajes privados, asumiendo el rol en esta ocasión de terceros conectados a la red que "leen" las comunicaciones de otros. El juego termina cuando uno de los grupos descifra el mensaje.

El propósito del juego es poner de manifiesto que los métodos de encriptación permiten que tengan acceso a la información solo quienes poseen la clave.

Antes de empezar los docentes aclaran que los mensajes se envían en mayúscula, que no hay espacios entre palabras y no usan el carácter **Ñ.**

Iteración 1:

1. **Carga del programa de adivinanza por el grupo emisor:** Quien oficie de emisor carga el programa microbit-cifrado-cesar-js-1.hex en su placa. El mensaje es "HOLAMUNDO" y está cifrado con un corrimiento de 4 caracteres.
2. **Instrucciones de carga:** El DR solicita a los estudiantes que realicen el siguiente programa para que las placas reciban los mensajes:



3. **Instrucciones de uso:** El DR comenta que cada grupo recibirá el mismo mensaje que está cifrado usando el Código César. Pero solo uno de ellos tendrá la clave de cifrado. La misión de todos es descifrar el mensaje.
4. **Descifrado:** Esta vez, el DA le va a dar la clave de cifrado a uno de los grupos (clave 4) y el otro grupo intentará descifrar el mensaje sin la clave.
5. **Descifrado:** Enviar el mensaje a las microbits usando el botón "A"

6. **Respuestas:** El primer equipo en descifrar el mensaje lo anuncia.

Iteración 2:
Se repite la dinámica anterior. En este caso, el programa a cargar es microbit-cifrado-césar-js-2.hex, el mensaje es "BUENDIADIA" y está cifrado con un corrimiento de 6 caracteres. Además, el DA debe darle la clave de cifrado al otro grupo (clave 6) y el grupo que tuvo la clave la iteración anterior intentará descifrar el mensaje sin ella. **Reflexión:** *¿Quiénes pudieron descifrar cada mensaje? ¿Por qué?*

3. Cierre (10 min)

Los docentes realizan una puesta en común para reflexionar sobre la importancia de la encriptación en las tecnologías digitales y la función de las computadoras en el encriptado de información.

¿En qué cosas de la vida diaria les parece que está presente la criptografía? ¿En qué situaciones les parece necesario que la información esté encriptada ? ¿Por qué? ¿Qué pasaría si no existiera el encriptado en Internet?

¿Se imagina si tuviéramos que encriptar y desencriptar a mano cada comunicación en internet?

El DR repone de ser necesario, 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.

Para anticipar el desafío de la próxima VC, puede plantearse la pregunta: *¿Podríamos descifrar el mensaje aunque no tuviéramos la clave?*

Registro en Crea

Registro en crea las respuestas a los enigmas y la pista descubierta. Publicación de notas grupales.

La Yapa: Propuestas para seguir en casa

Si querés saber más sobre la Criptografía en nuestra vida cotidiana podés ver este video

Los Códigos Secretos de la Historia - Los Creadores

ETAPA 3 ↓
Cierre

El objetivo de esta etapa es poner de manifiesto que los esquemas de criptografía se pueden romper y que, para esto, son particularmente útiles las computadoras. Como conclusión del proyecto se señala que ningún método de encriptación es infalible (aunque hay algunos mucho más resistentes que el César) y que además, en la seguridad de la información también son fundamentales las acciones humanas.

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 un programa de computadora. Los estudiantes observan que, a pesar de ser una tarea tediosa para realizar a mano, puede resolverse rápidamente con una 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 sin clave.
- Relativizar la seguridad de la información, tanto por el método de cifrado elegido como con 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 que dudas surgieron sobre el cierre del informe.

AULA ↓
Gestión de la información

Propósitos mínimos

- Analizar entre todos el 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

- Organizar una campaña escolar de sensibilización sobre la seguridad de la información en internet.

Notas para el DA ↓

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 3.
Esta actividad se problematiza en el inicio de la VC.

Para dicha campaña es posible trabajar con afiches, podcast, presentaciones, videos, juegos, etc.

VC ↓
Descifrando con computadoras

💡 Desafío
Descifrar mensajes sin conocer la clave.

1. Inicio (5 min)
El DR realiza una puesta en común del caso del profesor con el objetivo de analizar la actividad del aula.
¿Cómo les fue en la actividad? Si el profesor tenía sus datos cifrados ¿Que hubiese pasado? ¿Alcanza con cifrar la información para protegerla?
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 no se haya podido introducir Caso 1: Profesor de Historia en la clase de aula, se recomienda introducirlo brevemente al inicio de la VC.

2. Desarrollo (30 min)
Los docentes proponen otro juego de cifrado y descifrado.

Descifrando códigos 2
El objetivo de este juego es descifrar los mensajes que los docentes plantean.
Se sugiere enmarcar la actividad en una situación narrativa en la cual, los equipos receptores están “escuchando” el envío de mensajes privados, asumiendo el rol en esta ocasión de terceros conectados a la red y “leyendo” las comunicaciones de otros.

Iteración 1: Desciframos el mensaje sin computadora

1. **Mensaje inicial:** Los docentes comparten con el grupo un mensaje codificado, pero sin decir la clave, por ejemplo: *ehmzmqeqde* (*adivinanza* usando un corrimiento de 4 caracteres). **Es importante que el corrimiento sea bajo para que lo encuentren fácilmente al probar con la rueda.**

📌 Atención:
Los estudiantes en la próxima iteración descifrarán usando la página Calculadora en línea: Cifrado Cesar se sugiere cifrar los mensaje utilizando esta página para mantener estable el método que van a usar.
En este caso ROT4 equivale a un corrimiento de 4 caracteres

2. **Descifrado:** Se les sugiere a los estudiantes usar la rueda de cifrado que contiene la letra Ñ (ver anexo 2), usando esta rueda, escriban todas las posibilidades de descifrado que hay, haciendo una lista. En algún momento encontrarán un mensaje con sentido. **Resultados:** *¿Encontraron el mensaje cifrado? ¿Fue fácil? ¿Ayudó la rueda? ¿De cuantos lugares es el corrimiento?*

Iteración 2: Desciframos usando la computadora

1. **Mensaje inicial:** Los docentes comparten con el grupo un mensaje codificado sin compartir la clave, por ejemplo: *WCZMUXJ WYNUM* (*CIFRADO CÉSAR* usando un corrimiento de 22 caracteres). En este caso, el corrimiento debe ser alto, para reforzar la diferencia con el descifrado manual.

2. **Descifrado**: Esta vez se les sugiere a los estudiantes usar la página Calculadora en línea: Cifrado César para descifrar el mensaje.
3. **Resultados:** *¿Encontraron el mensaje cifrado? ¿Fue fácil? ¿Ayudó la página? ¿Por qué?*
4. **Otra vuelta:** Se repite la iteración con otro mensaje.
5. **Reflexión:** Se realiza una puesta en común para analizar las debilidades del cifrado César y poner de manifiesto el rol de las computadoras en el proceso de romper el código.
   ¿Es fácil de descifrar este cifrado? ¿Por qué? ¿Cuál es su debilidad? Si puedo calcular rápidamente todas las posibilidades de sustitución ¿Es importante la clave de cifrado? ¿Servirá este cifrado para enviar datos por la red? ¿Cuál es la diferencia entre usar la página y la rueda? ¿Por qué?

3. Cierre (10 min)

A partir de la dinámica de cierre que los docentes acuerden, se habilita un espacio de reflexión sobre las ventajas que ofrecen las computadoras en los procesos de cifrado descifrado con clave y sin clave.

¿Facilitó la computadora el descifrado sin la clave? ¿Por qué? ¿Qué ventajas tiene utilizar la computadora para cifrar o descifrar? ¿Qué rol cumplen las computadoras en este proceso? ¿Servirá este método para enviar información de manera segura en Internet?

Este contexto permite enunciar la existencia de otros métodos de seguridad (gpg, llave pública y privada, encriptado asimétrico, certificados, vpn, etc) que son lo que se utilizan en la actualidad, que si bien son más complejos de cifrar son tan difíciles de romper que, aún utilizando computadoras, no es factible encontrar la clave en un tiempo razonable.

Registro en Crea

Registro en crea las respuestas a los enigmas y la pis
descubierta. Publicación de notas grupales.

📑 ANEXO 1
Bebras: Código Secreto

1. Descifrar un mensaje:
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 última consonante,
la Z se cambia por la A.
Cómo escribiría el castor “HACEME UNA LLAMADA” usando este código secreto

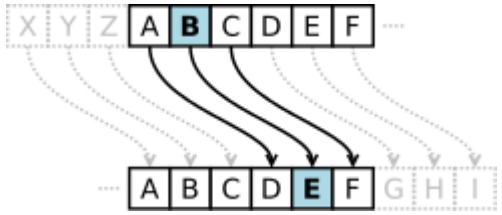
A: IAFEOE PA ÑÑAOAFA
B: TAYEUE UÑA IIAUAEA
C: JAVEQE UZA QQAMARA
D: IBDFNF VÑB MMBNBEB

Respuesta: D
La H se convierte en I la A en B, la C se convierte en D y así sucesivamente.

2. Cifrar un mensaje:
Usando el código de el castor y la liebre: Enviar un mensaje encriptado a un compañero.

📑 ANEXO 2
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



1. En este mensaje codificado, las letras se reemplazaron con otras letras, utiliza el código para descifrarlo:

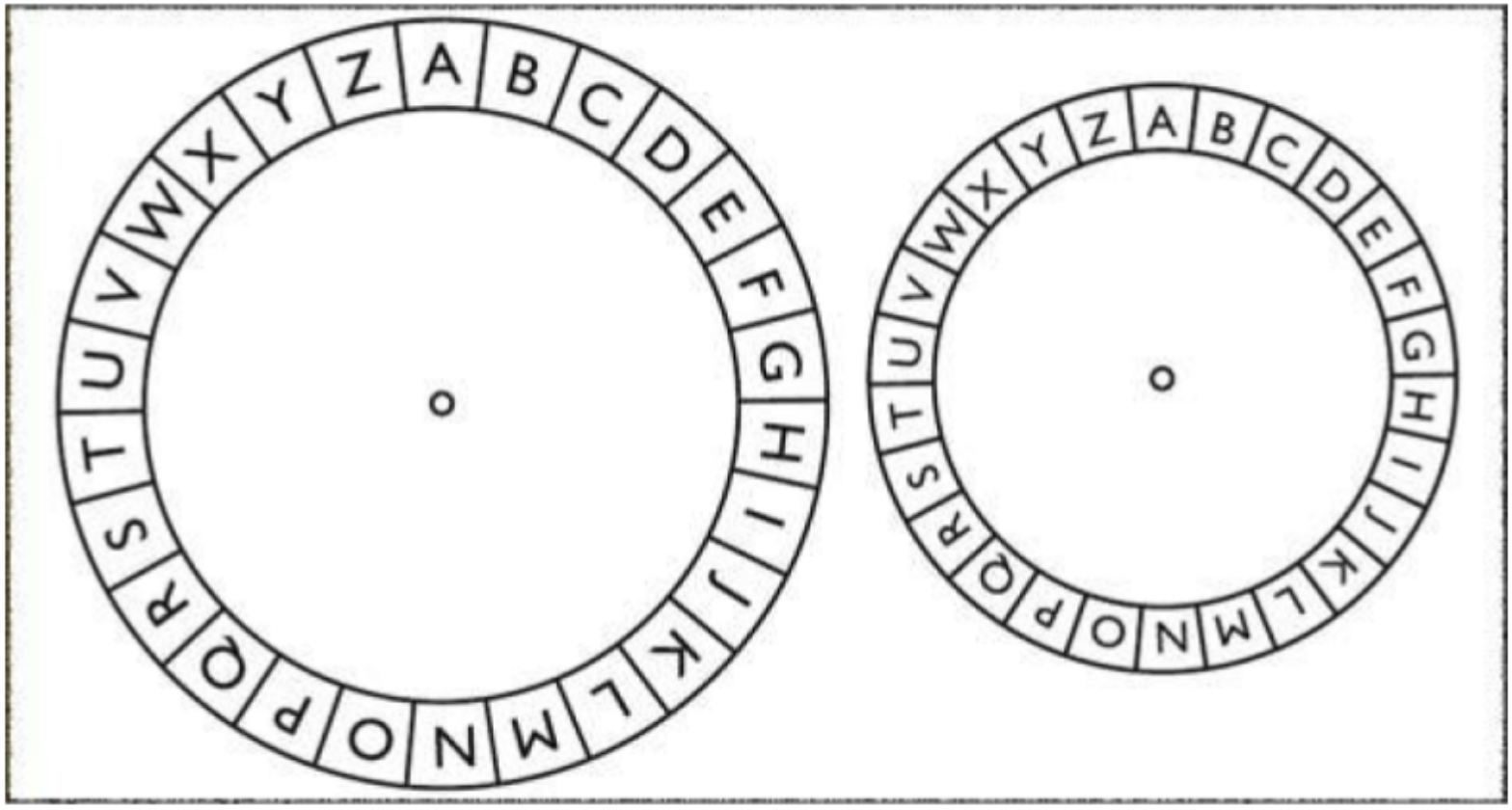
Mensaje Cifrado:	ÑHPWR HV PRUODÑ
Mensaje descifrado :	_ _ _ _ _ _ _ _ _ _ _ _ _ _ _

Código																								
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
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

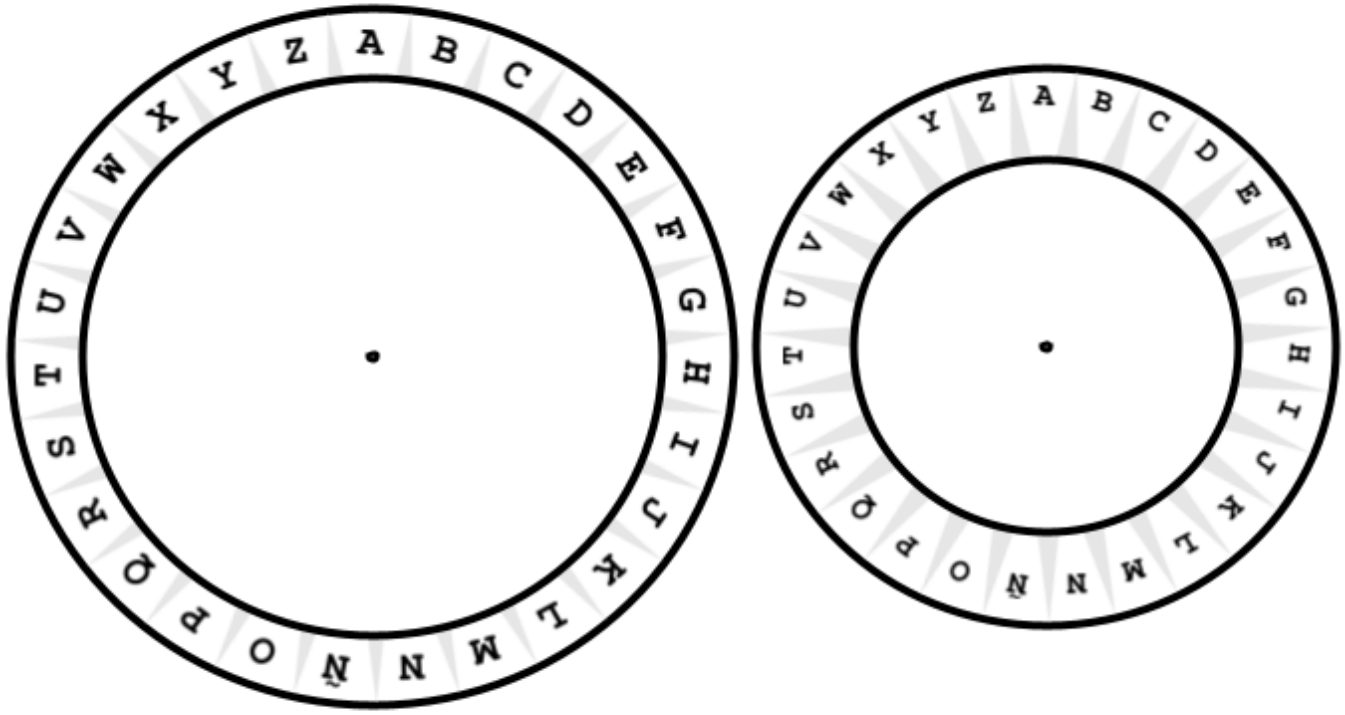
2. Envíale un mensaje cifrado a otro equipo

3. Descifra el mensaje que te envía un equipo.

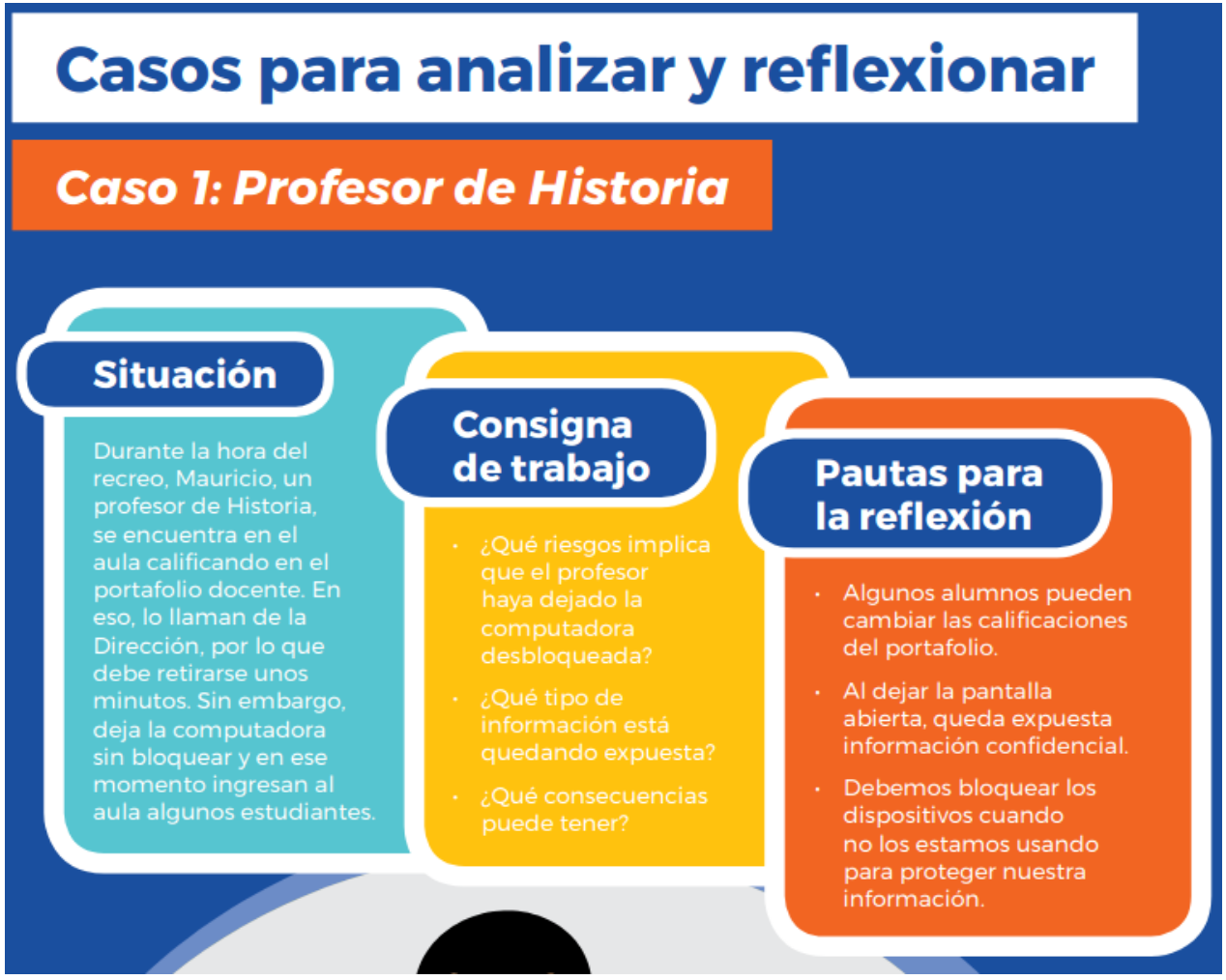
Podés usar estas plantilla para armar tu cifrado César



Plantilla con letra Ñ



📑 ANEXO 3
Gestión de la información



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