

# Desafío Contraseña



**TIEMPO:** 60 minutos.



**MATERIALES:** tizas o cinta de papel, lapicera, hojas de papel.



**POBLACIÓN SUGERIDA:** actividad pensada para docentes y estudiantes de educación media.



**ciudadanía  
digital**

*Escaneá el QR  
para acceder a  
la versión digital  
de otros recursos  
didácticos.*



## Habilidades de la Estrategia de Ciudadanía Digital sobre las cuales trabaja:

Manejo de la privacidad.

Manejo de riesgos.

El juego consiste, por un lado, en adivinar la contraseña secreta antes que otros grupos y, por otro lado, generar una contraseña lo más segura posible.

Como tercer propósito se trabaja sobre la utilidad de las contraseñas seguras y la necesidad de que sean personales y fáciles de memorizar.



### Preparación:

Para desarrollar esta actividad recomendamos elegir un lugar amplio que permita el movimiento, puede ser el patio o un salón despejado.

Se divide al grupo en 3 equipos.

Armar en el piso un cuadrante de 6 x 6 cuadrados, de 50 centímetros cada uno aproximadamente. Completar la primera columna con letras y la última fila con números.

Ejemplo de cómo armar el cuadrante:

E					
D					
C					
B					
A					
	1	2	3	4	5

Replicar este cuadrante en una hoja A4 por cada grupo con el que se defina realizar esta actividad.



**Desarrollo:**

- 1. Se divide al grupo en tres equipos: @, # y Ñ
- 2. Al grupo @ se le entrega una hoja con el cuadrante para que construya una contraseña de 10 dígitos con la premisa de que en cada fila señalada con letras deben haber dos caracteres.

Ejemplo:

E			5		ñ
D	A	2			
C		3		F	
B			t		a
A		P		a	
	1	2	3	4	5

Los grupos # y Ñ deberán adivinar la contraseña de la siguiente manera:

- 1. Se disputa con piedra, papel y tijera el grupo que comienza. Quien gana empieza.
- 2. Los grupos saben que por cada fila hay dos caracteres que deben adivinar antes de pasar a la siguiente fila. Quien adivina primero el último de la fila E gana.
- 3. El grupo ganador se pone de acuerdo donde comienza la primera persona del grupo que entra a la tabla del piso donde no hay información. Ejemplo: el grupo Ñ ganó y envía a una persona a pararse en el cuadrante “A1”, en este caso el grupo que armó el código les indica que es incorrecto. Entonces, es el turno de # que envía a una persona al cuadrante “A4”. Como el grupo acertó escribe en el piso el carácter que colocó el grupo del código en el piso (en este caso una “a”) y tiene otro turno. La persona se mueve al cuadrante “A2” y el grupo le dice que es correcto. Se escribe en el piso el carácter señalado y ahora el grupo puede avanzar a la fila de B. Una persona se para sobre “B2”. Al ser incorrecto el turno vuelve a ser de Ñ, y así sucesivamente hasta que un grupo descubra el último carácter.

- a. En esta etapa recibe 10 puntos el grupo que descubrió el último carácter de E.
  - b. Suma 10 puntos el grupo que descubrió más caracteres. Se recomienda ir anotando al correr de cada ronda qué grupo descubre cada carácter para sumar al final.
  - c. El grupo que escribió el código gana 10 puntos si su contraseña es segura, o sea, cumple con las siguientes reglas:
    - i. Tiene por lo menos 8 dígitos (en este caso se definen 10 para el juego).
    - ii. Tiene mayúsculas y minúsculas.
    - iii. Tiene símbolos y números.
4. Rotan los roles: # pasa a escribir el código y @ y Ñ compiten. Cuando se adivina el segundo carácter de E se contabilizan los puntos.
  5. En la tercera ronda vuelven a rotar los roles: Ñ arma el código y # y @ compiten.
  6. Al finalizar, se suman los puntos y se ofrece una última posibilidad de sumar 20 puntos. Se colocan las 3 contraseñas elaboradas para el juego en el siguiente sitio [Kaspersky Password Manager](#). La contraseña más segura será aquella que requirió más tiempo en ser descifrada.

### Ejemplo de puntaje:

	Ronda 1	Ronda 2	Ronda 3	Puntaje del link	Total
@	10 por generar una contraseña segura.	10 por llegar primero.	No sumó puntos en esta ronda.	20 puntos por ser la contraseña más difícil.	40 puntos.
#	10 por llegar primero y 10 por descubrir más caracteres	10 por generar una contraseña segura.	10 por llegar primero y 10 por adivinar más caracteres.	No suma puntos.	50 puntos.
Ñ	No sumó puntos en esta ronda.	10 por descubrir más caracteres.	Su contraseña no es segura, no suma puntos.	No suma puntos.	10 puntos.

Como cierre del proceso invitamos a dialogar en torno a las contraseñas que usan, si son seguras o no, lo que resguardan y sobre todo la necesidad de que una contraseña sea igualmente segura como recordable.

Para construir una buena contraseña, se puede realizar el ejercicio de pensar en algo que nos gusta mucho, como un lugar, un deporte, una comida o una canción, y transformarla.

- ♦ “Cancha de fútbol” podría ser una buena contraseña si la transformamos enC@nCH@d3futb0L
- ♦ “Vamo arriba bo!” se puede transformar en: VAW0ArrI8ab0!

Esta dinámica permite trabajar el valor de proteger información sensible, datos o accesos que se quieren resguardar, mediante una contraseña segura y que se puede memorizar.

### **Variaciones sugeridas:**

#### **Variante 1:**

Cuando un grupo acierta un cuadrante esta información no se escribe en el piso sino que tienen que recordarla. Esto complejiza la experiencia.

#### **Variante 2:**

Para hacerla más corta se puede dividir al grupo en 2. Uno crea la contraseña y otro trata de adivinar. Ahí lleva los puntos quien adivine la contraseña del grupo opuesto en la menor cantidad de intentos. Los puntos se suman por menor cantidad de intentos, contraseña segura y tiempo que lleve descifrar la contraseña en la página sugerida.



<b>Tarea entregable para obtener el puntaje:</b> Documento con fotos de los códigos y al menos 3 reflexiones de los chiquilines sobre lo aprendido.
<b>Comentarios y/ u observaciones:</b>

**Ejemplo de documento entregable**

<b>Institución:</b>	<b>Grupo:</b>
<b>Foto de los códigos (contraseñas) armados por cada grupo que jugó.</b>	
<b>Reflexiones que se desprenden del proceso:</b>  1.    2.    3.	