DEPARTAMENTO DE
INGENIERÍA
INFORMÁTICA
UNIVERSIDAD DE SANTIAGO DE CHILE

GUÍA 4.2

10145 - FUNDAMENTOS DE PROGRAMACIÓN PARA INGENIERÍA
10110 - FUNDAMENTOS DE COMPUTACIÓN Y PROGRAMACIÓN

Ejercicios

INTRUCCIONES GENERALES

- Cree un **.py** con su **RUN** como nombre del archivo.
- Agregue como encabezado del programa los siguientes datos:

```
# FUNDAMENTOS DE PROGRAMACIÓN PARA INGENIERÍA/FUNDAMENTOS DE COMPUTACIÓN Y PROGRAMACIÓN
# SECCIÓN DEL CURSO:
# PROFESOR DE TEORÍA:
# PROFESOR DE LABORATORIO:
#
# AUTOR
# NOMBRE:
# RUN:
# CARRERA:
```

Ejercicio 4.2

- Utilizando el **revisador - estudiante 4.2**

- En la era digital en la que vivimos, la seguridad en línea es más importante que nunca. Las contraseñas son una de las principales medidas de seguridad que se utilizan para proteger nuestras cuentas en línea. Sin embargo, muchas personas no toman en serio la seguridad de sus contraseñas, lo que puede poner en peligro no solo su propia información personal, sino también la información de otras personas.

- Los riesgos de tener una contraseña vulnerable son muchos. Un atacante puede robar una contraseña débil para acceder a una cuenta y robar información personal, como nombres, direcciones, números de teléfono, direcciones de correo electrónico y contraseñas de otras cuentas. En casos más graves, los atacantes pueden atacar esas contraseñas débiles para acceder a información confidencial, como datos bancarios o de tarjetas de crédito.

Ejercicio 4.2

- Se le solicita crear un programa que reciba una contraseña utilizando el mensaje "**`Ingrese su pass:`** " y validar que cumpla los siguientes criterios:

- Debe tener un largo de ocho caracteres exactos. Si no cumple, debe mostrar solamente el siguiente mensaje y terminar:
  - **`"Debe tener 8 caracteres."`**

- Una vez validado eso debe comprobar la composición de la contraseña, validando que posea al menos una minúscula, una mayúscula, una letra, un dígito, una coma y un punto y coma. En caso no cumplir estos criterios, debe mostrar los siguientes mensajes, según corresponda en el orden presentado:
  - **`"Debe tener al menos una minúscula."`**
  - **`"Debe tener al menos una mayúscula."`**
  - **`"Debe tener al menos una letra."`**
  - **`"Debe tener al menos un dígito."`**
  - **`"Debe tener al menos una coma."`**
  - **`"Debe tener al menos una punto y coma."`**
- En caso de cumplir todos los criterios descritos, debe mostrar el mensaje:
  - **`"Su password cumple con todas las reglas."`**

- Nota: El problema presentado es con fines pedagógicos, por lo que se redujo la cantidad de caracteres a trabajar a solo 8 para no extender demasiado el desarrollo. Cabe destacar que a 2024 la obtención de una contraseña con 8 caracteres que contenga minúsculas, mayúsculas, números y símbolos se estima en unos 40 minutos, por lo que se recomienda contraseñas más largas y utilizar un segundo factor de autentificación.

¿CONSULTAS?