Instrucciones de uso para el Sistema de creación y acceso de usuarios - CMD

Instalación:

En el archivo README.md disponible en el repositorio se encuentran los pasos a seguir para la instalación y puesta en funcionamiento del programa.

Instrucciones de uso:

Una vez instalado correctamente, para ejecutar el programa se ingresa por línea de comando

$ *ruby cmd.rb*

para ejecutarlo.

Valores por defecto:

Al ejecutarse, el programa tiene los siguientes valores por defecto:

1. Usuario: el programa crea un usuario con el nombre **admin** y la clave **admin**
2. Método de encriptación: por defecto es el método de Texto Plano
3. Sesión: no hay usuario con sesión iniciada

Menú principal:

Menú sin sesión activa:

El menú principal informa primero el tipo de encriptación utilizada actualmente y luego presenta las opciones, al iniciar el programa no hay sesión activa y las opciones son las siguientes:

Tipo de encriptación: Texto Plano
1. Ingresar
2. Crear_Usuario
3. Cambiar_Encriptación
4. Estado
5. Salir
?

Elija la opción que desee ingresando el número y apretando enter.

1. Ingresar : Se utiliza para crear una sesión con un usuario existente. Se deberá ingresar el usuario y la clave correspondiente para poder ingresar. En caso de error en alguno de los dos, se producirá un error y no podrá iniciarse sesión.

Importante: el nombre del usuario puede contener letras, números y los caracteres – (guión) _ (guión bajo) y . (punto). Debe ser de al menos cuatro caracteres para ser válido.

A su vez, las claves ingresadas deben tener también al menos cuatro caracteres, y los caracteres permitidos varían según el tipo de encriptación. (Ver: **Tipos de encriptación**)

2. Crear Usuario: Crea un nuevo usuario. Para ello, se debe ingresar el usuario y la clave dos veces. Las dos claves ingresadas deben ser iguales. En caso de no coincidir las dos claves iniciadas, no podrá crearse el usuario. La consola mostrará las siguientes líneas:

Ingrese el usuario:
Ingrese clave:
Confirme la clave:

Importante: el nombre del usuario puede contener letras, números y los caracteres – (guión) _ (guión bajo) y . (punto). Debe ser de al menos cuatro caracteres para ser válido.

A su vez, las claves ingresadas deben tener también al menos cuatro caracteres, y los caracteres permitidos varían según el tipo de encriptación. (Ver: **Tipos de encriptación**)

3. CambiarEncriptación: Cambia el tipo de encriptación que utiliza el sistema para almacenar las claves. Las opciones son: Texto Plano, Caesar's Cypher y Bcrypt. Muestra un submenú para elegir entre dichas encriptaciones:

1. Texto_Plano
2. Caesars_Cypher
3. BCrypt
?

Elija la opción que desee ingresando el número y apretando enter.

Importante: El cambio de tipo de encriptación **no se efectúa** sobre las claves de los usuarios ya existentes, por lo tanto si se desea ingresar con un usuario con otro tipo de encriptación, debe volver a cambiarse la misma a la que corresponda.

4. Estado: Muestra su estado actual en el programa, a saber: si se inició sesión con algún usuario mostrará el mensaje:

Su sesión está activa con el usuario: <usuario>

Si no se inició sesión, se mostrará:

Usted no ha iniciado sesión

5.Salir: Sale del programa. Si hay una sesión iniciada, la cierra antes de salir.

Menú con sesión activa:

1. Cerrar_Sesión
2. Cambiar_Encriptación
3. Estado
4. Salir
?

Las opciones tienen el mismo funcionamiento, a excepción de:

1. Cerrar Sesión: cierra la sesión activa actualmente

4. Salir: cerrará la sesión antes de salir del programa

Tipos de encriptación:

Los distintos tipos de encriptación para las claves aceptan distintos caracteres en las claves de los usuarios, y funcionan de distintas maneras:

Texto Plano: La clave es guardada en memoria tal como fue enviada. Es el método menos seguro. Los caracteres aceptados son: letras, números y los caracteres – (guión) _ (guión bajo) y . (punto). Debe ser de al menos cuatro caracteres para ser válido.

Caesar's Cypher: La clave es encriptada antes de ser guardada en memoria, luego se desencripta para compararla con la clave enviada por el usuario que quiere ingresar. Es más seguro que el Texto Plano. Los caracteres aceptados son letras solamente, mayúsculas o minúsculas. Debe ser de al menos cuatro letras para ser válido.

Bcrypt: La La clave es encriptada antes de ser guardada en memoria, luego se compara con la clave enviada por el usuario que quiere ingresar mediante un método propio del sistema de encriptación. Es el método más seguro de todos. Los caracteres aceptados son: letras, números y los caracteres – (guión) _ (guión bajo) y . (punto). Debe ser de al menos cuatro caracteres para ser válido.