**Manual de Usuario: Generador de**

**Claves de Alta Seguridad (v2.0)**

**1. Introducción y Propósito**

**Bienvenido al GCR-20. Esta herramienta ha sido diseñada para solucionar el problema de crear contraseñas que sean matemáticamente seguras (difíciles de hackear) pero cognitivamente accesibles (posibles de recordar).**

**El sistema toma una palabra de su elección y la transforma en una "Super Clave" estandarizada de hasta 20 caracteres, mezclando mayúsculas, números y símbolos especiales.**

**2. Requisitos del Sistema**

**Para ejecutar esta herramienta, asegúrese de cumplir con lo siguiente:**

- **Sistema Operativo: Windows 10/11, macOS, o Linux.**
- **Entorno: Python 3.6 o superior instalado.**
- **Teclado: Estándar (la herramienta acepta caracteres alfanuméricos).**

**3. Guía de Inicio Rápido**

**Paso 1: Ejecutar la aplicación**

**Abra su terminal o consola de comandos y ejecute el script. Verá el siguiente mensaje de bienvenida parpadeando en el cursor:**

**Ingrese una palabra para su clave:**

**Paso 2: Ingresar la "Semilla" (Input)**

**Escriba una palabra que sea significativa para usted.**

- ***Ejemplo:* Barcelona**
- **Nota: El sistema convertirá automáticamente su texto a MAYÚSCULAS.**

**Paso 3: Obtener la Clave**

**Presione ENTER. El sistema procesará la información instantáneamente y mostrará:**

1. **La clave segura generada.**
2. **La longitud final de la clave (generalmente 20 caracteres).**

**4. Análisis Profundo: ¿Cómo funciona mi nueva clave?**

**A diferencia de otros generadores, este sistema no es totalmente aleatorio. Utiliza una arquitectura de Segmentación y Relleno.**

**Reglas de Procesamiento Automático**

**El sistema aplica las siguientes reglas a lo que usted escriba:**

1. **La Regla del 9: El sistema solo tomará las primeras 9 letras de su palabra.**
    - ***Si escribe:*** **SUPERCOMPUTADORA (16 letras)**
    - ***El sistema lee:*** **SUPERCOMP (9 letras)**
    - ***Por qué:*** **Esto se hace para dejar espacio suficiente para insertar los códigos de seguridad.**
2. **La Estructura de Bloques: La contraseña final se divide en 3 secciones separadas por guiones. Cada sección contiene Ruido Aleatorio seguido de Su Palabra.**

**Esquema Visual:**

**[RUIDO + PARTE1] - [RUIDO + PARTE2] - [RUIDO + PARTE3]**

**Ejemplo Práctico de Lectura**

**Si su palabra clave fue HOLA: El sistema generará algo como: %$9HO-a2wL-..0A**

- **Bloque 1: %$9HO -> Ruido (%$9) + Su letra (HO)**
- **Bloque 2: a2wL -> Ruido (a2w) + Su letra (L)**
- **Bloque 3: ..0A -> Ruido (..0) + Su letra (A)**

**Consejo de memorización: Usted solo necesita recordar la palabra "HOLA". Los caracteres extraños que están *antes* de sus letras son escudos de seguridad generados por la máquina.**

**5. Comportamiento ante Entradas (Casos de Uso)**

**Aquí explicamos qué hace el programa dependiendo de lo que usted escriba:**

| Situación | Entrada del Usuario | Resultado del Sistema | Explicación |
|---|---|---|---|
| Palabra Corta | SOL | Mucho "ruido" aleatorio. | Al ser la palabra corta, el sistema agrega más símbolos para llegar a los 20 caracteres. |
| Palabra Larga | ESTERNOCLEIDOMASTOIDEO | Se corta en la 9na letra. | El sistema usará ESTERNOCL y agregará poco ruido. |
| Números | 123456 | Clave mixta válida. | Los números son tratados como texto y se mezclan con símbolos. |
| Símbolos | P@$$w0rd | Clave muy compleja. | El sistema acepta símbolos en la entrada y agrega MÁS símbolos. |

**6. Solución de Problemas (Troubleshooting)**

Problema: La contraseña generada tiene menos de 20 caracteres (ej: 19).

- Causa: Esto es normal debido a la división matemática interna. Si los espacios no se pueden dividir exactamente entre 3, el sistema redondea hacia abajo.
- Solución: No se requiere acción. Una clave de 18 o 19 caracteres sigue siendo extremadamente segura.

Problema: La contraseña tiene caracteres extraños como \, |, { o }.

- Causa: El sistema usa string.punctuation, que incluye todos los símbolos especiales del teclado ASCII.
- Solución: Si algún sitio web no acepta estos símbolos, puede borrarlos manualmente o generar una nueva clave ejecutando el programa otra vez.

Problema: Copié la contraseña, pero el sitio web dice "Formato inválido".

- Causa: Algunos sitios viejos no aceptan guiones (-) o espacios.
- Solución: Borre los guiones que separan los bloques. La seguridad de la clave se mantiene intacta.

**7. Aviso de Seguridad y Responsabilidad**

1. Aleatoriedad: Cada vez que ejecuta el programa, la clave cambia (incluso si usa la misma palabra). Anote su clave inmediatamente, ya que no hay forma de recuperarla si cierra el programa.
2. Entropía: Esta herramienta utiliza caracteres alfanuméricos y signos de puntuación, lo que eleva la entropía (dificultad de adivinanza) a niveles aptos para banca y correos electrónicos.
3. Privacidad: El código se ejecuta localmente en su máquina. Ninguna contraseña es enviada a internet ni guardada en bases de datos externas.

**8. CONCLUSIONES PARA EL USUARIO**

Al finalizar esta guía y comenzar a utilizar el Generador GCR-20, podemos concluir lo siguiente sobre su seguridad digital:

1. Seguridad sin Estrés: Ha eliminado la necesidad de elegir entre una contraseña *fácil de recordar* (pero insegura) y una *imposible de adivinar* (pero difícil de memorizar). Con esta herramienta, obtiene lo mejor de ambos mundos: su palabra favorita protegida por una armadura matemática.
2. Protección Proactiva: Al usar contraseñas de 20 caracteres con símbolos y números, usted se coloca por encima del 99% de los usuarios de internet, haciendo que sus cuentas sean objetivos extremadamente difíciles y costosos para los ciberdelincuentes.

3. Privacidad Total: A diferencia de los generadores de claves en páginas web (online), esta herramienta funciona 100% en su computadora. Nadie, ni siquiera los creadores del software, tiene acceso a las claves que usted genera.
4. El Factor Humano: Recuerde que la herramienta es solo la mitad del trabajo. La otra mitad depende de usted: guardar la clave en un lugar seguro y nunca compartirla con desconocidos.

## 9. REFERENCIAS Y RECURSOS RECOMENDADOS


**Bitwarden Inc.** (2024). *Bitwarden: Open Source Password Manager*. Recuperado el 8 de diciembre de 2024, de https://bitwarden.com/

**Hunt, T.** (s.f.). *Have I Been Pwned: Check if your email or phone is in a data breach*. Recuperado el 8 de diciembre de 2024, de https://haveibeenpwned.com/

**Instituto Nacional de Ciberseguridad (INCIBE).** (2023). *Guía de ciberseguridad para usuarios: Gestión de contraseñas seguras*. Oficina de Seguridad del Internauta (OSI). https://www.osi.es/es/guia-de-ciberseguridad

**National Institute of Standards and Technology (NIST).** (2017). *Digital Identity Guidelines: Authentication and Lifecycle Management* (NIST Special Publication 800-63B). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-63b

**Security.org.** (2024). *How Secure Is My Password? Tool and Analysis*. Recuperado el 8 de diciembre de 2024, de https://www.security.org/how-secure-is-my-password/