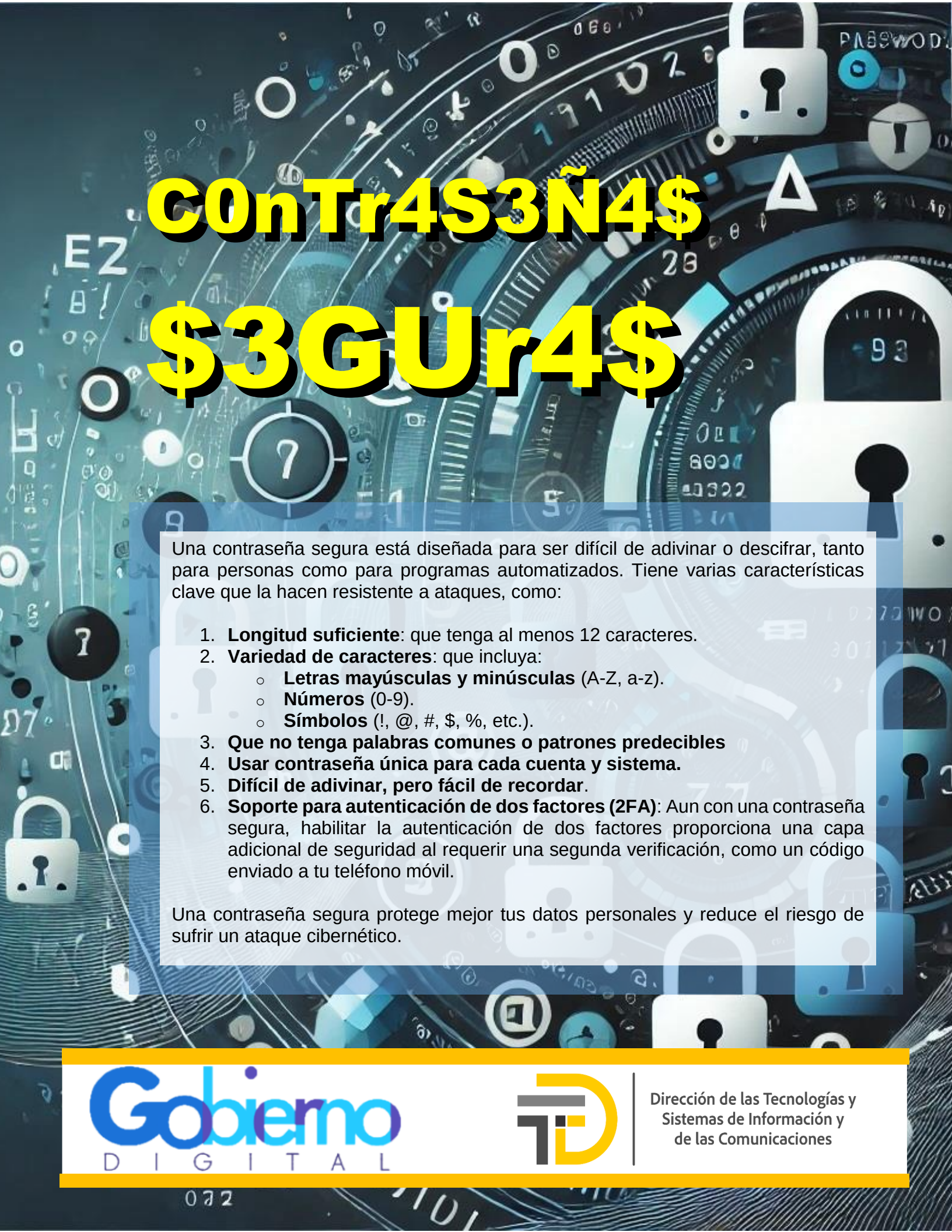

Una contraseña segura está diseñada para ser difícil de adivinar o descifrar, tanto para personas como para programas automatizados. Tiene varias características clave que la hacen resistente a ataques, como:

1. **Longitud suficiente**: que tenga al menos 12 caracteres.
2. **Variedad de caracteres**: que incluya:
   - **Letras mayúsculas y minúsculas** (A-Z, a-z).
   - **Números** (0-9).
   - **Símbolos** (!, @, #, $, %, etc.).
3. **Que no tenga palabras comunes o patrones predecibles**
4. **Usar contraseña única para cada cuenta y sistema.**
5. **Difícil de adivinar, pero fácil de recordar**.
6. **Soporte para autenticación de dos factores (2FA)**: Aun con una contraseña segura, habilitar la autenticación de dos factores proporciona una capa adicional de seguridad al requerir una segunda verificación, como un código enviado a tu teléfono móvil.

Una contraseña segura protege mejor tus datos personales y reduce el riesgo de sufrir un ataque cibernético.

Gobierno DIGITAL

Dirección de las Tecnologías y Sistemas de Información y de las Comunicaciones

COMO LAS ADIVINAN

Los programas automatizados diseñados para adivinar contraseñas utilizan diversas técnicas para intentar descifrar contraseñas, suelen aprovechar la debilidad de las contraseñas cortas, simples o comunes, para usar métodos y técnicas como:

1. Ataques de fuerza bruta Es la prueba y error de todas las combinaciones posibles hasta encontrar la contraseña correcta mediante la combinación simples y corta, de palabras comunes a sus preferencias, nombres y números relacionados.

2. Ataques de diccionario Se conoce esta técnica por el uso de palabras comunes como "password", "123456" o "qwerty", “admin” se basa en el hecho de que muchas personas usan contraseñas comunes o palabras del diccionario con combinaciones simples como “Gato123”.

3. Ataques de combinaciones y variaciones (Hybrid Attack) Es la combinación de palabras relacionadas con su perfil agregando variaciones de caracteres como el cambio de letras por símbolos o números por letras como, por ejemplo, "P@ssw0rd"

4. Ataques por patrones del teclado El software intenta combinaciones basadas en cómo las personas suelen teclear, lo que puede incluir patrones horizontales o diagonales en el teclado como por ejemplo qwerty, asdfg, 1qaz2ws,

5. Ataques basados en filtraciones de contraseñas (Credential Stuffing) Cuando las personas usan la misma contraseña para varios accesos y en uno de esos fue capturada es probada en varios sistemas y cuentas. los atacantes obtienen una base de datos de contraseñas filtradas (de una brecha de seguridad), pueden usar esas contraseñas en otros sitios.

6. Ataques de ingeniería social Los programas pueden aprovechar datos personales disponibles en línea para probar contraseñas relacionadas con información conocida (como nombres de mascotas, fechas de cumpleaños, etc.).

7. Ataques de diccionario extendido (Rainbow Tables) Las contraseñas en muchos sistemas se almacenan están en forma de "hash", que es una representación cifrada. Los atacantes utilizan estas tablas para encontrar una coincidencia entre el hash de la contraseña y las combinaciones precomputadas.

Para evitar que los programas automatizados descifren tus contraseñas, es importante seguir buenas prácticas como usar contraseñas largas, complejas y únicas, y habilitar la autenticación de dos factores (2FA).

Gobierno DIGITAL

Dirección de las Tecnologías y Sistemas de Información y de las Comunicaciones

CONSEJOS PARA CREAR UNA CONTRASEÑA

1. **Longitud mínima de 12 caracteres**: Cuanto más larga sea la contraseña, más difícil será descifrarla.
2. **Combine diferentes tipos de caracteres**:
   - **Letras mayúsculas y minúsculas** (A-Z, a-z).
   - **Números** (0-9).
   - **Símbolos** (!, @, #, $, %, etc.).
3. **Evite palabras comunes y fáciles de adivinar**: No uses palabras de diccionario, nombres propios, fechas de nacimiento o secuencias obvias como "12345" o "password".
4. **Use frases o combinaciones aleatorias**: Una estrategia efectiva es usar una frase que no tenga sentido, como "PerroVerde!Camina#Rápido32", o mezclar varias palabras sin relación.
5. **No reutilice contraseñas**: Cada cuenta debe tener una contraseña única para evitar que, si una cuenta es comprometida, todas las demás cuentas también lo sean.
6. **Utilice un gestor de contraseñas**: Si le cuesta recordar múltiples contraseñas, un gestor de contraseñas puede generar y almacenar contraseñas fuertes, de manera segura.
7. **Habilita la autenticación de dos factores (2FA)**: Siempre que sea posible, habilite esta opción. Es una capa adicional de seguridad que requiere un código de verificación además de la contraseña.
8. **Evite patrones en el teclado**: No use combinaciones de teclas que sigan patrones visibles, como "qwerty" o "asdfg".

Gobierno DIGITAL

Dirección de las Tecnologías y Sistemas de Información y de las Comunicaciones