

Artículo

[Dmitry Maslennikov](#) · Mayo 16 Lectura de 3 min

[Open Exchange](#)

¿ Cómo de segura es una contraseña?

¿ Cómo podemos comprobar si una contraseña es suficientemente segura, para evitar que sea descifrada? ¿ Y cómo podemos crear una contraseña segura?

He desarrollado una herramienta que puede ayudar con esto. Puedes encontrarla en [OpenExchange](#). Instálala con zpm

```
zpm "install passwords-tool"
```

Este módulo instalará solo una clase caretdev.Passwords, que contiene algunos métodos que pueden ayudarte.

Contraseña segura

Para crear una contraseña segura, normalmente es suficiente con usar letras en mayúsculas y minúsculas, números y símbolos especiales, y que tenga al menos 8 caracteres.

Método Generate con parámetros

- Length - longitud de la contraseña generada, valor 12 por defecto
- IncludeUpperLetter - Incluir letras ASCII en mayúsculas, 2 si se requiere, 1 por defecto
- IncludeLowerLetter - Incluir letras ASCII en minúsculas, 2 si se requiere, 2 por defecto
- IncludeNumber - Incluir números, 2 si se requiere, 1 por defecto
- IncludeSymbol - Incluir símbolos especiales, 2 si se requiere, 1 por defecto

```
USER>w ##class(caretdev.Passwords).Generate(12,1,0,0,0)
FMXRQEQPOVBC
USER>w ##class(caretdev.Passwords).Generate(12,1,1,0,0)
rgbPyWApcUjp
USER>w ##class(caretdev.Passwords).Generate(12,1,1,1,0)
cDuLf8FqEDx7
USER>w ##class(caretdev.Passwords).Generate(12,1,1,1,1)
0J/ 1LbW|T$
USER>w ##class(caretdev.Passwords).Generate(
w3}{OQA|T{h^
```

En vez del [\\$random](#) habitual, que puede no ser tan seguro para contraseñas, este método utiliza `$System.Encryption.GenCryptRand()`. Además de obtener mejores contraseñas, genera unas pocas contraseñas en un bucle, comprueba su entropía y devuelve una con la calificación más alta.

Entropía

La entropía de una contraseña predice cómo de difícil será descifrar una contraseña dada, a través de ataques de fuerza bruta, ataques de diccionario u otros métodos comunes. Básicamente, la entropía mide cuántos intentos necesitará hacer un atacante para adivinar una contraseña. Hay varias formas de calcularla.

```
USER>write ##class(caretdev.Passwords).Entropy("Pas$W0rD")
52.56
```

Fórmula de la entropía

L = Longitud de la contraseña; Número de símbolos en la contraseña

S = Tamaño del conjunto de símbolos únicos posibles (rango de caracteres disponibles).

Por ejemplo:

Números (0-9): 10

Alfabeto latino en minúsculas (a-z): 26

Alfabeto latino en minúsculas y mayúsculas (a-z, A-Z): 52

Conjunto de caracteres ASCII Imprimibles (a-z, A-Z, símbolos, espacio): 95

Número de Combinaciones Posibles = S^*L

Entropía = $\log_2(\text{Número de Combinaciones Posibles})$

Entropía de Shannon

```
USER>write ##class(caretdev.Passwords).ShannonScore("Pas$W0rD")
24
```

Esta forma se basa en la frecuencia de uso de caracteres y en la longitud de la contraseña. Más detalles en la [Wikipedia](#) (en inglés).

Clasificación NIST

```
USER>write ##class(caretdev.Passwords).NISTScore("Pas$W0rD")
24
```

Cálculo

- La entropía del primer caracter es cuatro bits;
- La entropía de los siete caracteres siguientes son dos bits por caracter;
- Los caracteres del noveno al vigésimo tienen 1.5 bits de entropía por caracter;
- Los caracteres 21 y siguientes tienen un bit de entropía por caracter.
- Se añade un "bonus" de seis bits si se usan tanto letras en mayúscula como caracteres no alfabéticos.
- Se añade un "bonus" de seis bits para contraseñas con longitud de 1 a 19 caracteres después de una exhaustiva comprobación en el diccionario para asegurar que la contraseña no está incluida en un diccionario completo. Contraseñas de 20 caracteres o más no reciben este bonus porque se asume que son frases de contraseña que consisten en múltiples palabras del diccionario.

Fuerza

```
write ##class(caretdev.Passwords).DetermineStrength("Pas$W0rD")
REASONABLE
```

Y contraseña generada

```
USER>write ##class(caretdev.Passwords).DetermineStrength(##class(caretdev.Passwords).
Generate())
STRONG
```

- VERY_WEAK - Entropía ≤ 32
- WEAK - Entropía ≤ 48
- REASONABLE - Entropía ≤ 64

- STRONG - Entropía ≤ 80
- VERY_STRONG - Entropía > 80

Espero que os resulte útil.

[#Seguridad #InterSystems IRIS](#)

[Compruebe la aplicación relacionada en InterSystems Open Exchange](#)

URL de fuente: <https://es.community.intersystems.com/post/%C2%BFc%C3%B3mo-de-segura-es-una-contrase%C3%B1a>