

Método de Creación de Contraseñas Robustas "deThi4-go"

Índice

1- Introducción	2
=== deThia4-go simple ===.....	3
=== deThia4-go variable ===	4
=== deThia4-go variable compleja ===.....	5
=== deThia4-go super variable compleja ===	7
=== Resumen de los 4 métodos deThia4-go ===	9
=== Ejemplos Aplicados al método deThia4-go ===	9
=== Ejemplos AVANZADOS y VARIABLES aplicados al método deThia4-go === ..	11
2- Créditos	12

Método de Creación de Contraseñas Robustas "deThi4-go"

1- Introducción

Este método para crear contraseñas, es muy simple y la complejidad de la contraseña ira variando -haciéndose más compleja- a medida que vayamos avanzando en la creación y variedad de diseño de la password.

Nuestro método aplica al procedimiento de autenticación "Single sign on", más un agregado, que en este caso lo llamaremos "**FACTOR deThi4-go**".

Recordamos que Single sign-on (SSO) es un procedimiento de autenticación de usuarios, en el cual una misma contraseña se utiliza para ingresar o loguearse ante varios sistemas, aplicaciones, correos electrónicos, etc.

Siempre debemos tener en cuenta que crear una contraseña robusta nos hace menos vulnerables a recibir cualquier tipo de ataque a la misma.

Esta forma de crear contraseñas – el método "**deThi4-go**", es recomendable de implementar cuando tenemos que recordar muchas de ellas (se supone que una persona común no tiene menos de 8 (ocho) contraseñas). No obstante, no hay reparo en que se utilicen para uno, dos o pocos sitios en los cuales tengamos que autenticarnos con una password.

Dependiendo del rebuscamiento al momento de crear o modificar la contraseña, el método "**deThi4-go**", clasifica de la siguiente manera sus distintos niveles de realización:

- * deThia4-go simple
- * deThia4-go variable
- * deThia4-go variable compleja
- * deThia4-go super variable compleja

A todos estos niveles, le podremos agregar una variación adicional llamada precisamente **AVANZADA** y **VARIABLE**, de manera de robustecer cualquiera de las cuatro alternativas del método presentado. Esta explicación se desarrolla al final del presente documento.

MUY IMPORTANTE: En todos los casos, la longitud mínima de la password será de 10 (diez) caracteres.

=== deThia4-go simple ===

La formación de este tipo de contraseñas se basa en que la misma debe tener al menos la siguiente estructura:

Nota: Primero mostraremos el ejemplo y luego se explicará su desarrollo para un mejor entendimiento.

Password: batman71@+

En donde:

** 1er paso: una palabra que puede ser conocida. Aquí "batman"

** 2do paso: una cifra. Aquí "71"

** 3er paso: un símbolo. Aquí "@"

** 4to paso: un símbolo del teclado numérico. Aquí "+"

*** Con todos estos pasos realizados, nos faltaría agregar el 5to y último, que denominamos "**FACTOR deThi4-go**".

Si yo poseo n+1 cantidad de passwords para los servicios de correo electrónico, foros, banca on line, servicios asociados y todos los que se me ocurra suscribirme, voy a crear una contraseña para todos estos usuarios siguiendo los pasos 1 a 4 del método "deThia4-go".

Ahora -siguiendo el ejemplo- ya cree mi "Single Sign On" denominado en este caso **batman71@+**.

Luego –en este caso-, voy a crear la password para mi correo electrónico de Gmail, utilizando el "metodo deThia4-go" + el "FACTOR deThi4-go"; [siendo en este caso el "FACTOR deThi4-go" la inicial de Gmail = g](#).

Finalmente la password: batman71@+g

Siguiendo con este método, tendremos, por ejemplo:

Para mi cuenta Wikipedia: batman71@+w

Para mi cuenta Yahoo: batman71@+y

Para mi cuenta Hotmail: batman71@+h

Para mi cuenta Skype: batman71@+s

Para mi cuenta home banking: batman71@+hb -por ser dos palabras el servicio original de referencia-.

.... Y así indefinidamente podríamos seguir creando contraseñas para dispositivos electrónicos, teléfonos, computadoras, netbooks, notebooks, etc. Por ejemplo:

Para mi notebook: batman71@+n

Para mi iPad: batman71@+i

Para mi AP (Access Point): batman71@+ap

Podemos definir entonces al "'FACTOR deThi4-go'", como el caracter -ya sea una letra, un número o un símbolo-, o el conjunto de caracteres, que me diferenciara en los distintos accesos de passwords a los diferentes sistemas, aplicaciones, correos electrónicos, foros, blogs, banca on line, dispositivos, teléfonos inteligentes, routers, etc., etc., etc., que necesite una contraseña para ser accedido.

Aclaración 1: Puede ser que alguna vez, servicios que utilicen en este caso la inicial de la aplicación o dispositivos, tengan la misma password. En este caso no habrá inconvenientes ya que los ingresos para esos sistemas o equipos serán distintos, pero una vez que utilicemos seguidamente este método de construcción de passwords, claramente podremos variar la formación de la contraseña -como veremos más adelante- utilizando en algunos casos la letra inicial, en otros la final, y así en forma indistinta de ubicación, produciendo la desigualdad de mismas contraseñas.

Aclaración 2: El paso 2 “una cifra. Aquí "71"”, hace referencia a una cifra de 2 (dos) dígitos, aquí no hay limite en cantidad de números a ingresar en este paso, pudiéndose agregar tantos números como creamos necesarios y que éste número sea fácil de recordar sin necesidad de anotarlo en ningún lugar.

Aclaración 3: Cuando hablamos de utilizar un símbolo del teclado numérico, no solo nos referimos al teclado tradicional de PC, que lo tiene incorporado sobre la derecha del mismo, también nos referimos a utilizar en las notebooks la combinación de teclas “Fn” + el símbolo que queramos, en los smartphones la combinación de teclas “alt” + el símbolo que queramos y así con cada dispositivo que utilicemos.

Aclaración 4: Cuando estamos realizando el “4to paso: un símbolo del teclado numérico. Aquí "+””, según el ejemplo mostrado, hacemos referencia a utilizar uno de los símbolos que encontramos en este teclado numérico como podría ser el ., +, -, * o /; de manera de identificar rápidamente una tecla de este mini-teclado. No obstante ello, dependiendo de la práctica que tengamos en componer este tipo de contraseñas, nada impide que utilicemos las teclas numéricas (0,1, 2, 3, 4, 5, 6, 7, 8 o 9) en vez de los símbolos.

=== deThia4-go variable ===

La formación de este tipo de contraseñas se basa en que la misma debe tener al menos la siguiente estructura:

Nota: Primero mostraremos el ejemplo y luego se explicará su desarrollo para un mejor entendimiento.

Password original: batman@71+

En donde:

** 1er paso: una palabra que puede ser conocida. Aquí "batman"

** 2do paso: una cifra. Aquí "71"

** 3er paso: un símbolo. Aquí "@"

** 4to paso: un símbolo del teclado numérico. Aquí "+"

** 5to paso: "FACTOR deThi4-go".

** 6to paso: hasta aquí los 5 pasos anteriores son los mismos que en el método "deThia4-go simple", el variable, de esta versión me indica que, respetando los cinco primeros pasos necesarios para la creación de la contraseña; el 6to paso hará que deje establecido en el final el "FACTOR deThi4-go", pero cambie el orden de formación de la password.

En este caso, alterando el orden de los pasos y, siendo "g" el "FACTOR deThi4-go" algunas de las siguientes combinaciones de password para elegir podrían ser; para este ejemplo de un usuario en Gmail:

Password: "71batman@+g" o

Password: "batman@+71g" o

Password: "71@batman+g" o

Password: "+batman@71g" y más.

Hasta que no hayamos ganado experiencia con este tipo password, es conveniente mezclar el orden de los pasos de la formación de la misma ("deThia4-go variable"), pero NO del "FACTOR deThi4-go".

Para empezar a utilizar el método "deThia4-go variable", cambiando la ubicación del "FACTOR deThi4-go" pasando a la primer posición de la contraseña, le recomendamos como una buena práctica de uso, utilizar el método " deThia4-go variable" con el "FACTOR deThi4-go" como último caracter para cuentas de usuario de servicios y el método "deThia4-go variable" con el "FACTOR deThi4-go" como primer caracter para cuentas o logins de dispositivos electrónicos.

=== deThia4-go variable compleja ===

De similar estructura de construcción que " deThia4-go simple" y " deThia4-go variable".

La única variación que incorporamos aquí, es que - el 1er paso: una palabra que puede ser conocida, como ejemplo "batman" - se forma con una combinación de las distintas técnicas de creación de password conocidas, aplicándose entonces:

- **Forme acrónimos fáciles de recordar para usted:**

Por Ejemplo:

"verpersos" perteneciente a combinar "Verón, Perez, Sosa" - grandes jugadores de fútbol.

"bonedgmul" perteneciente a combinar "Bono, Edge, Muller" - grandes músicos.

"fatkolcha" perteneciente a combinar "Fatiga, Koller, Chaleco" - apodos de mis amigos.

- **Mezcle una frase reconocida por usted de su inventiva o una frase popular, canción, libro, película, etc.**

Por ejemplo:

"semequelca" perteneciente a combinar "se me quedó el catamarán" - frase propia utilizada diariamente.

"volvalfutu" perteneciente a combinar "volver al futuro" - gran película de cine.

"elmedeve" perteneciente a combinar "El mercader de Venecia" - gran libro de Shakespeare.

Estas son solo algunas de las técnicas más conocidas y fáciles de recordar para mejorar la fortaleza de una password.

En estos ejemplos se tomaron -generalmente- las 2 (dos) primeras letras de cada palabra, pero de acuerdo a como nos vayamos familiarizando con esta forma de crear acrónimos y mezclar frases, podremos avanzar a utilizar frases más largas y tomar menos o más letras de cada una de ellas.

Para formar una password "deThia4-go variable compleja", repetimos como siempre, los pasos 1 a 5.

Por ejemplo, desmenuzando la clave para Gmail **verpersos71@+g**, nos queda que:

** 1er paso: una palabra que puede ser conocida. Aquí "verpersos"

** 2do paso: una cifra. Aquí "71"

** 3er paso: un símbolo. Aquí "@"

** 4to paso: un símbolo del teclado numérico. Aquí "+"

** 5to paso: "FACTOR deThi4-go". Aquí g (perteneciente a Gmail)

Podríamos decir que **verpersos71@+g**, es la versión más simple del método "deThia4-go variable compleja".

Empezando a utilizar variables de contraseñas con esta metodología podríamos obtener como ejemplo:

Password: verpersos@71+g
Password: @verpersos71+g

Password: g@verpersos71+

Password: g+@verpersos71

Password: 71verpersos+g@ y más.

=== deThia4-go super variable compleja ===

De similar estructura de construcción que "deThia4-go variable compleja". La variable que incorporamos aquí, es que - "el 1er paso: una palabra que puede ser conocida, como ejemplo "batman" - se deben reemplazar letras por números o símbolos, de acuerdo a como queramos o nos resulte más sencillo reemplazar y recordar las letras que hemos reemplazado en la palabra original.

Podríamos hacer mentalmente una tabla de reemplazos de letras, en dónde:

la letra a o A sean reemplazadas por el número 4.

la letra e o E sean reemplazadas por el número 3.

la letra i o I sean reemplazadas por el número 1.

la letra o u 0 sean reemplazadas por el número 0.

la letra s o S sean reemplazadas por el número 5.

Otros reemplazos podrían ser:

la letra g o G sean reemplazadas por el número 6.

la letra t o T sean reemplazadas por el número 7.

la letra q o Q sean reemplazadas por el número 2.

la letra b o B sean reemplazadas por el número 8.

También podríamos reemplazar así en forma combinada de números y letras por símbolos:

la letra o u 0 sean reemplazadas por el símbolo *.

la letra l o L sean reemplazadas por el símbolo (.

la letra i o I sean reemplazadas por el símbolo !.

la letra b o B sean reemplazadas por el símbolo {.

El número 7 sea reemplazado por el símbolo /

El número 2 sea reemplazado por el símbolo ?

Como vemos, podemos armar tablas de reemplazos de letras, números y símbolos de la forma que se nos ocurra, siempre de manera tal que lo podamos recordar mentalmente y no nos veamos obligados a dejar escrita esta "tabla" de conversión de caracteres en algún sitio en donde nos la puedan encontrar.

De acuerdo a alguna de las tablas que hemos expuesto, ejemplos de palabras y sus reemplazos serían:

Para BATMAN = B4tm4n

Para batman = 8a7man

Para telefonito = t3l3f0n1t0

Para bolsillo = {0(5!((0

Para contenedor = c*nt3n3d*r y más.

A partir de la "tabla" de reemplazos de caracteres que hayamos elegido para la palabra o "frase" de nuestra contraseña, construimos la password con los pasos 1 a 5 del método "deThia4-go".

Para formar una password "deThia4-go super variable compleja", repetimos como siempre, los pasos 1 a 5

Para el siguiente ejemplo vamos a reemplazar en la clave verpersos:

-> El número **3** por la letra **e** o **E** y el número **0** por la letra **o** u **O**.

Al fin, desmenuzando la clave para Gmail **v3rp3rs0s71@+g** (de la original verpersos@71+g), nos queda que:

** 1er paso: una palabra que puede ser conocida. Aquí "v3rp3rs0s"

** 2do paso: una cifra. Aquí "71"

** 3er paso: un símbolo. Aquí "@"

** 4to paso: un símbolo del teclado numérico. Aquí "+"

** 5to paso: "FACTOR deThi4-go". Aquí g (perteneciente a Gmail)

Podríamos decir que **v3rp3rs0s71@+g**, es la versión más simple del método "deThia4-go super variable compleja".

Empezando a utilizar variables de contraseñas con esta metodología podríamos obtener como ejemplo:

Password: v3rp3rs0ss@71+g

Password: @v3rp3rs0s71+g

Password: g@v3rp3rs0s71+

Password: g+@v3rp3rs0s71

Password: 71v3rp3rs0sg+@ y más.

=== Resumen de los 4 métodos deThia4-go ===

Finalmente, con algo de tiempo para practicar -no mucho- podremos utilizar claves más complejas con este método de creación de password o contraseñas conocido como "deThi4-go", un método muy útil para recordar una gran cantidad de ellas y difícil de descifrar por parte de **los ataques de diccionario** y eventuales ataques de **Ingeniería social**.

En resumen:

Ejemplo de una password para una cuenta de usuario de Gmail, con los cuatro métodos vistos.

-> deThia4-go simple = Password: **batman71@+**

-> deThia4-go variable = Password: **71batman@+g**

-> deThia4-go variable compleja = Password: **g@verpersos71+**

-> deThia4-go super variable compleja = Password: **v3rp3rs0ss@71+g**

=== Ejemplos Aplicados al método deThia4-go ===

Todos los ejemplos son para un usuario con 10 passwords de cuentas de:

""Ejemplo aplicado simple""	""Ejemplo aplicado variable""
Wikipedia: batman71@+w	Wikipedia: 71batman@+w
Gmail: batman71@+g	Gmail: 71batman@+g
Yahoo: batman71@+y	Yahoo: 71batman@+y
Hotmail: batman71@+h	Hotmail: 71batman@+h
Home Banking: batman71@+hb	Home Banking: 71batman@+hb
Twitter: batman71@+t	Twitter: 71batman@+t
Facebook: batman71@+f	Facebook: 71batman@+f
Google+: batman71@+g+	Google+: 71batman@+g+
Mercadolibre: batman71@+ml	Mercadolibre: 71batman@+ml
Notebook: batman71@+n	Notebook: 71batman@+n

""Ejemplo aplicado variable complejo""	""Ejemplo aplicado súper variable complejo""
Wikipedia: w@verpersos71+	Wikipedia: v3rp3rs0ss@71+w
Gmail: g@verpersos71+	Gmail: v3rp3rs0ss@71+g
Yahoo: y@verpersos71+	Yahoo: v3rp3rs0ss@71+y
Hotmail: h@verpersos71+	Hotmail: v3rp3rs0ss@71+h
Home Banking: hb@verpersos71+	Home Banking: v3rp3rs0ss@71+hb
Twitter: t@verpersos71+	Twitter: v3rp3rs0ss@71+t
Facebook: f@verpersos71+	Facebook: v3rp3rs0ss@71+f
Google+: g+@verpersos71+	Google+: v3rp3rs0ss@71+g+
Mercadolibre: ml@verpersos71+	Mercadolibre: v3rp3rs0ss@71+ml
Notebook: n@verpersos71+	Notebook: v3rp3rs0ss@71+n

=== Ejemplos AVANZADOS y VARIABLES aplicados al método deThia4-go ===

Después de cierto tiempo y práctica de haber realizado contraseñas aplicando cualquiera de las cuatro variaciones [deThia4-go simple](#), [deThia4-go variable](#), [deThia4-go variable compleja](#) o [deThia4-go super variable compleja](#), estaremos en condiciones de agregar más caracteres en algunos, todos o uno de los pasos que conformar la contraseña, principalmente y sobretodo fácilmente sobre el "FACTOR deThi4-go".

El "FACTOR deThi4-go", para la contraseña de Wikipedia que inicialmente era la letra "w" por ser la inicial podría complejizarse de las siguientes maneras:

Contraseña inicial: Wikipedia -> **batman71@+w**

Con [deThia4-go simple Avanzada](#) y [Variable de Wikipedia](#) podría ser:

Wikipedia tomando las letras **Wikipedia** nos queda -> **batman71@+wk**

Wikipedia tomando las letras **Wikipedia** nos queda -> **batman71@+wpd**

Wikipedia tomando las letras **Wikipedia** nos queda -> **batman71@+wka**

Wikipedia tomando las letras **Wikipedia** nos queda -> **batman71@+wkpa**

[Podríamos tomar la inicial y solo las vocales.](#)

Wikipedia tomando las letras **Wikipedia** nos queda -> **batman71@+wiieia**

[Podríamos tomar la inicial y solo las consonantes.](#)

Wikipedia tomando las letras **Wikipedia** nos queda -> **batman71@+wkpd**

Como vemos en todos los ejemplos, una vez establecido el método y las variaciones que vayamos a utilizar, la forma de componer la contraseña se hace muy fácil de crear, de recordar y a la vez es bastante difícil de descifrar.

En resumen:

Ejemplo de una password para una cuenta de usuario Wikipedia, con los cuatro métodos vistos + AVANZADOS y VARIABLES.

-> deThia4-go simple = Password: **batman71@+wkpd**

-> deThia4-go variable = Password: **71batman@+ wkpd**

-> deThia4-go variable compleja = Password: **wkpd @verpersos71+**

-> deThia4-go super variable compleja = Password: **v3rp3rs0ss@71+ wkpd**

Si aún deseamos, podemos hacer más compleja la password, agregando una cifra de más números en el “paso 2”. Por ejemplo:

- Mi número de documento 32.273.218
 - agregándole 2 números más a cada cifra para no delatarme: 54495430.
 - agregándole 2 números menos a cada cifra para no delatarme: 10051096.
 - agregándole 1 número más a la primer división (32), 2 números más a la segunda división (273) y 3 números más a la tercer división: 43495541.
 - agregándole 1 número menos a la primer división (32), 2 números menos a la segunda división (273) y 3 números menos a la tercer división: 21051985.

Tomando uno de los casos mencionados arriba, tendríamos que para cada ejemplo:

-> deThia4-go simple = Password: **batman43495541@+wkpd**

-> deThia4-go variable = Password: **43495541batman@+ wkpd**

-> deThia4-go variable compleja = Password: **wkpd @verpersos43495541+**

-> deThia4-go super variable compleja = Password: **v3rp3rs0ss@43495541+ wkpd**

2- Créditos

Autor:	Damián Ienco (Ingeniero en Sistemas Informáticos)
Fecha de revisión actual:	17 de agosto de 2011
Fecha de revisión anterior:	12 de agosto de 2011
Nombre del documento:	Método de creación de contraseñas robustas “deThi4-go”
Contacto:	damianienco@gmail.com