# PMG - Un gestor de contraseñas generadas

Si sumamos [los datos de los distintos sitios de renombre cuyas identidades han sido expuestas obtenemos más de 161 millones](http://www.elladodelmal.com/2014/03/mas-de-161-millones-de-identidades.html). Es un número alarmante, pero [si no utilizas la misma contraseña en distintos sitios](http://www.elladodelmal.com/2010/10/reutilizacion-de-contrasenas.html), y además [utilizas Latch para controlar el acceso a tu cuenta](https://latch.elevenpaths.com/), puedes empezar a dormir tranquilo.

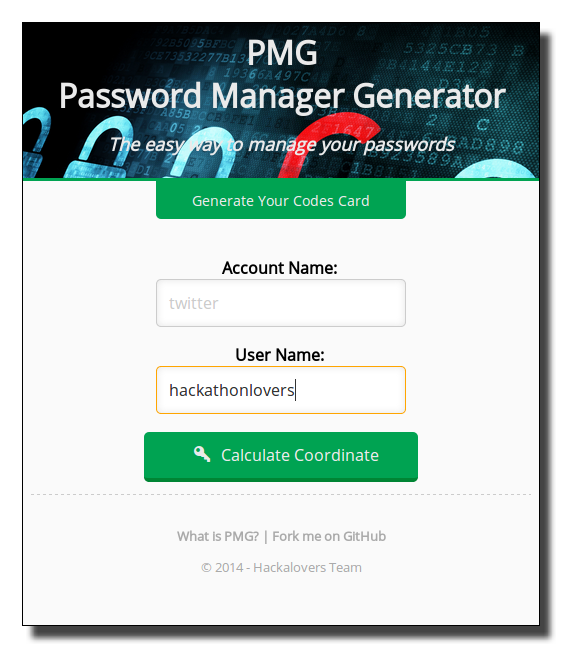
Latch se está empezando utilizar cada vez en más sitios, y para generar contraseñas robustas existen varios métodos. Podemos usar por ejemplo [el método "deThi4-go"](http://www.elladodelmal.com/2011/11/generacion-de-contrasenas-robustas-para.html). También podemos utilizar [bases de datos cifradas como KeepPass](http://keepass.info/). O también podemos utilizar [PMG, otro método para generar contraseñas robustas](http://pasmangen.github.io/), cuyas características, funcionamiento y manejo vamos a explicar a continuación.

## ¿Cómo funciona PMG?

El funcionamiento de PMG consiste en utilizar el nombre de tu cuenta, un código de seguridad y una contraseña maestra para **generar un hash que utilizaremos como contraseña** de dicha cuenta. Puede que así dicho, no se entienda muy bien, pero manejando la aplicación es como mejor se comprende, así que expliquemos como se usa.

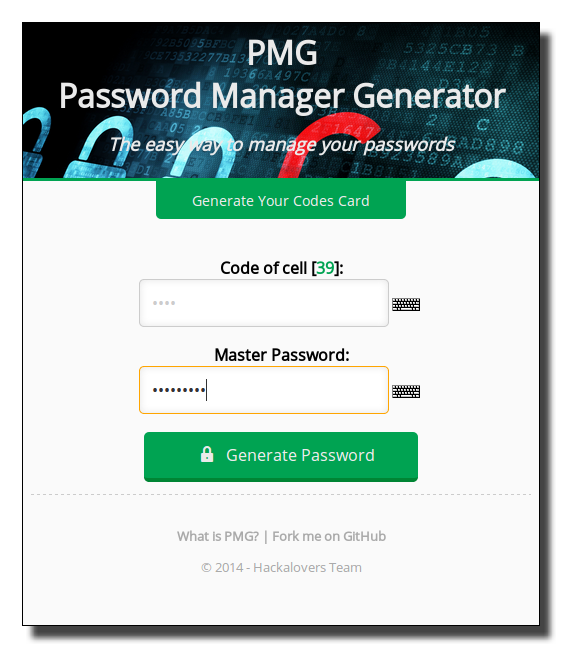
## ¿Cómo se usa PMG?

El uso de PMG es bastante sencillo. En la primera pantalla nos pide que introduzcamos el nombre de la cuenta (por ejemplo: twitter, gmail, etc.) y el nombre del usuario (por ejemplo: chemaalonso, hackathonlovers, etc.). Esto se pensó así para los que tienen distintos usuarios en un mismo servicio.



Los datos de nombre de la cuenta y nombre de usuario se guardan en el Local Storage del Navegador, para que en futuras utilizaciones nos aparezca un menú de autocompletar, para escribir menos y poder ir más rápidos.

Una vez rellenos los datos, pinchamos en el botón de "Calculate Coordinate", y entonces nos aparece otra pantalla donde tenemos que introducir un código de una tarjeta de coordenadas y una contraseña maestra.



La coordenada que se nos pide (en este caso la coordenada 39) va a ser siempre la misma para la tupla nombre de cuenta y nombre de usuario. De hecho se calcula normalizando los textos, sumando el valor numérico de cada carácter y calculando el módulo del número de coordenadas de la tarjeta, como puede apreciarse en la siguiente muestra de código:

var account = normalizeText( $('#account').val() );

var user = normalizeText( $('#user').val() );

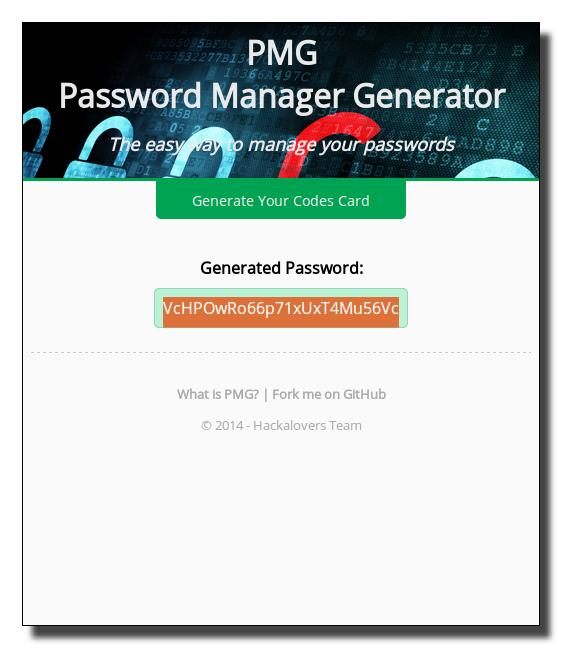
var data = account + user;

var dataCode = sumCharCode( data );

var coordenate = dataCode % CODES\_CARD\_CELLS;

El código de la tarjeta de coordenadas no es obligatorio ponerlo, aunque sí aconsejable para incrementar la seguridad. Un poco más abajo explicaremos cómo [crear nuestra propia tarjeta de coordenadas](#crear-tarjeta-coordenadas).

Tanto el código de tu tarjeta de coordenadas como tu contraseña maestra, se pueden introducir mediante un teclado virtual para evitar posibles keyloggers e incrementar aún más la seguridad. Una vez introducidos se mostrará la contraseña generada. Está última no se ve a simple vista, hay que seleccionarla para poder visualizarla y poder copiarla.



La contraseña generada va a ser siempre la misma para el conjunto de: nombre de cuenta, nombre de usuario, código de la tarjeta de coordenadas y contraseña maestra; pues es el hash del conjunto de datos. Se puede apreciar en la siguiente muestra de código:

var account = $('#account').val();

var user = $('#user').val();

var password = $('#password').val();

var code = $('#code').val();

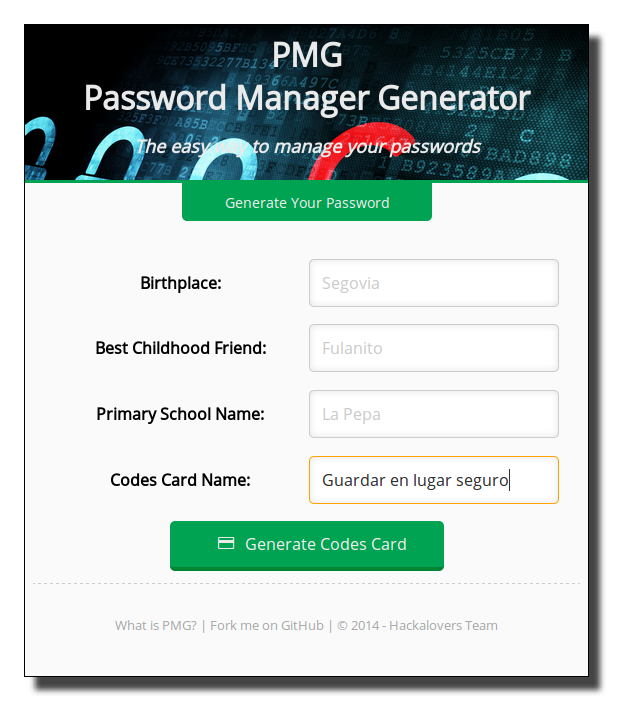
var data = normalizeText( account + user ) + code + password;

var hash = hashWrapper( data );

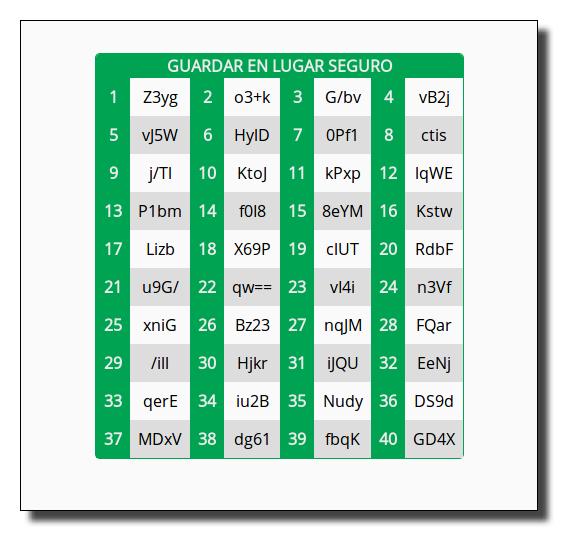
var generatedPassword = hash.substr( 0, GENERATED\_PASSWORD\_LENGTH );

## ¿Cómo crear tu propia tarjeta de coordenadas?

Como hemos dicho antes, aunque no es obligatorio, para incrementar la seguridad, PMG nos pide un código de una tarjeta de coordenadas. Si queremos usar esta característica, debemos de tener una tarjeta de coordenadas antes de empezar a usar PMG. Afortunadamente PMG te permite obtener la tuya propia. Para ello pinchamos en "Generate Your Codes Card" y nos muestra una pantalla en donde tendremos que rellenar ciertos datos.



Estos datos son: tu lugar de nacimiento, el nombre de tu mejor amigo de la infancia, el nombre de colegio de primaria. Como estos datos se pueden obtener mediante [ingeniería social](http://www.elladodelmal.com/2013/06/un-pequeno-juego-de-ingenieria-social.html), se ha añadido un campo más que es el nombre de tu tarjeta de coordenadas, que debería ser totalmente secreto. Una vez rellenados los campos, si pinchamos en el botón "Generate Codes Card" y obtendremos una tarjeta de coordenadas como la siguiente, que podremos imprimir:



Para los mismos datos introducidos, obtendremos siempre la misma tarjeta de coordenadas, puesto que nos muestra nada más y nada menos que un hash de dichos datos, como puede apreciarse en la siguiente muestra de código:

var birthplace = normalizeText( $('#birthplace').val() );

var childhoodFriend = normalizeText( $('#childhoodFriend').val() );

var schoolName = normalizeText( $('#schoolName').val() );

var cardName = normalizeText( $('#cardName').val() );

var data1 = birthplace + childhoodFriend + schoolName + cardName;

var data2 = schoolName + cardName + birthplace + childhoodFriend;

var hash = hashWrapper(data1) + hashWrapper(data2);

## Características de PMG

* PMG genera **contraseñas robustas y diferentes** para cada una de tus cuentas.
* PMG sólo te obliga a recordar **una contraseña maestra**.
* PMG permite incrementar la seguridad mediante el uso de una **tarjeta de coordenadas**.
* PMG no guarda ningún dato en la nube, **todo es generado en local**.
* PMG está totalmente desarrollado en **HTML, CSS y JavaScript**.
* PMG se puede usar tanto en el PC como en el móvil, **sólo te hace falta un navegador**.
* PMG tiene una licencia de **Softwre Libre** permisiva.

## ¿Cómo nació PMG?

Como buenos [amantes de los hackathones](http://www.meetup.com/Hackathon-Lovers/), Carlos Azaustre ([@carlosazaustre](http://twitter.com/carlosazaustre)), Jorge Arévalo ([@jorgeas80](http://twitter.com/jorgeas80)) y Adolfo Sanz De Diego ([@asanzdiego](http://twitter.com/carlosazaustre)) desarrollaron PMG durante el [I Hackathon del t3chfest](http://techfest.uc3m.es/concursos/hackathon/)