# CAI 1. CONSULTA SOBRE EL CUMPLIMIENTO DE POLÍTICAS DE SEGURIDAD DE CONTRASEÑAS


Escuela Técnica Superior de
**Ingeniería Informática**

# Índice



CONFIDENCIAL

# Alcance y Objetivos de la Auditoría

La importancia de la seguridad para empresas y estructuras informáticas no ha hecho más que aumentar a lo largo del tiempo. Bases de datos, usuarios y acceso, son parte del conjunto de elementos que precisan una protección adecuada, resistente y a la orden del día.

Como hemos ido viendo a lo largo de los años, ni las empresas tecnológicas más grandes y avanzadas del sector, llegan a librarse de fallas en su seguridad, que ponen en riesgo a miles de usuarios y datos internos.

Por ello, esta consultoría tiene como objetivo analizar, dar solución y comunicar a la empresa contratante, los fallos de seguridad presentes en los datos proporcionados

# Estudio Inicial

Como primera instancia de esta auditoría, debemos saber de que información disponemos, por tanto, expondremos los hashes en las siguiente tabla:

| Nombre del Usuario | Username | Hash de la Contraseña |
|---|---|---|
| Manuel Jimen Ventoyk | mjimenven | 26967c61a7f5442fb47861f812126ccf02a65bde |
| José María Quevedo Yuw | jmquevedo | b1b3773a05c0ed0176787a4f1574ff0075f7521e |
| Rafael Hidalgo Gasca | rhgasca | 35a9c2444ec63ee39f3b214edb9011f32e624a28 |

Una vez analizamos un poco la información de los hashes, podemos ver que se trata de un hash con una longitud de 40 caracteres hexadecimales, que se traducen a 160 bits, por tanto podemos intuir que se trata de un hash de tipo SHA-1.

## Estudio de las Tecnologías Adecuadas y Alternativas

En orden para estudiar la fortaleza de las contraseñas suministradas por la empresa, vamos a atacar usando las siguientes metodologías:

### Tabla Arcoíris

Una tablas arcoíris es un conjunto precalculados de valores hash, estas se basan en la colisión de hashes almacenando una gran cantidad de información en los dispositivos físicos. A pesar de ser bastante efectivas en un ámbito temporal, debido a la limitación de nuestros recursos, no podremos hacer uso de ellas por tanto nos decantaremos por las dos siguientes metodologías.

### Ataque de Diccionario

Los ataque de diccionario es un método de ataque en los que se usan grandes archivos de texto donde se almacenan como su nombre indica diccionarios de las palabras más usuales.

Es un gran método para encontrar contraseñas de uso común o muy sencillas, ademas para este hay multitud de opciones online, por ejemplo, Hashes.com, md5decrypt.net, o algunos con más opciones como dcode.fr, en el Anexo II podemos ver como usar la mayoría de estas herramientas. Aunque si queremos hacerlo con nuestros ordenadores, podemos usar programas como John the Ripper para Linux o Hash Suite y Hashcat para Windows, usando un diccionario adecuado siendo entre los más populares RockYou y un diccionario reciente como Koanashi.

### Fuerza Bruta

Su funcionamiento consiste en probar combinaciones de caracteres hasta encontrar aquella que de un resumen igual al buscado, debido a esto supone una carga computacional importante en función del número de caracteres y los caracteres que se hayan usado para crear-

CONFIDENCIAL

la, ya que no es lo mismo una clave numérica de 8 cifras a una de 4, teniendo $10^8$ y $10^4$ combinaciones respectivamente, y más aun con una clave alfanumérica que incluya los estándares mínimos descritos por la empresa donde el número de combinaciones sería $87^8 \approx 3.28e{+}15$.

Usaremos el programa de acceso libre Hashcat v6.1.1, que permite el desencriptado con fuerza bruta. Le proporcionaremos datos al algoritmo y este generará todas las combinaciones de caracteres que especifiquemos y sus respectivos resúmenes, hasta que se produzca una coincidencia con el resumen que estamos buscando.

# Recursos para la Auditoría

## Recursos Humanos

El equipo de seguridad para esta asignatura se compone de los siguientes miembros:

- Barragán Candel, Marina - estudiante de Ing. Informática – Tecnología Informática, en la mención de Tecnologías de la información
- Calcedo Vázquez, Ignacio - estudiante de Ing. Informática – Tecnología Informática, en la mención de Sistemas de Información
- Polo Domínguez, Jorge - estudiante de Ing. Informática – Ingeniería de Computadores
- Sala Mascort, Jaime Emilio - estudiante de Ing. Informática – Tecnología Informática, en la mención de Computación

## Recursos Tecnológicos

El equipo dispone de los siguientes dispositivos para realizar la auditoría:

- Ordenador 1, las características de este ordenador son:
  - Intel® Core™ i5-3570K
  - GTX 660 Ti OC 2GB GDDR5
  - RAM 8GB DDR3
  - SSD 500GB Samsung 860 EVO
- HP Pavilion x360,
  - Intel Core i5 8250U
  - Nvidia GeForce 940MX
  - 12 GB DDR4
  - HDD 1TB
- ASUSPRO P2520LA,
  - Intel Core i3-4005U
  - RAM 4GB DDR3L SODIMM
  - HDD 500GB
- HUAWEI MateBook D 14 AMD,
  - AMD Ryzen 5 3500U
  - Radeon™ Vega 8 Graphics
  - 8 GB DDR4
  - 512 GB PCIe SSD

CONFIDENCIAL

Las distintas actividades que se realizaran en esta auditoría serán las siguientes:

## Análisis de Hashes

Como se determinó en el estudio inicial, nos encontramos con hashes del tipo SHA1, en primer lugar se dio un barrido inicial con un ataque de diccionario, seguido de un ataque de fuerza bruta con el hash restante.

### Ataque de Diccionario

Gracias a este ataque, hemos podido hallar rápidamente dos de las tres contraseñas suministradas, correspondientes a Manuel Jimen Ventoyk y José María Quevedo Yuw, ofreciéndonos los resultados que aparecen en Consola 1.

```
qwerty           (jmquevedo)
vituperio        (mjimenven)
2g 0:00:00:05 DONE (2020-10-16 17:26) 0.3831g/s 2747Kp/s 2747Kc/s
3297KC/sie168..*7
```

*Consola 1: Output del programa John the Ripper con rockyou.txt*

Sin embargo, no pudimos hacer frente a uno de los hashes con este ataque, así que o bien el diccionario no era completo o bien no es una contraseña típica al uso.

### Ataque por Fuerza Bruta

Ya que uno de los hashes se resistió, procedimos a un ataque por fuerza bruta, haciendo uso en este caso de la herramienta Hashcat. Para ello se utilizaron distinto parámetros para agilizar la búsqueda:

- -m, para indicar que se trata de un hash del tipo SHA1
- -a, para indicar que se va a realizar un ataque por fuerza bruta
- ?1?1?1?1?1?1?1?1, para indicar el tamaño máximo de palabra, en este caso se optó por ocho, ya que asumimos que son contraseñas que no cumplían los requisitos mínimos y si los cumpliera, sería lo más pequeño posible
- -i, indica que estamos en modo incremento de máscara, donde se incrementa en 1 el número de caracteres definidos
- -1 rafelhidgosc?d, indica que cada uno de los ?1 pueden ser dígitos

Con esto se ha conseguido obtener la contraseña, aaeiao5, como se muestra en Consola 2.

CONFIDENCIAL

```
35a9c2444ec63ee39f3b214edb9011f32e624a28: aaeiao5
Session..........: hashcat
Status...........: Cracked
Hash.Name........: SHA1
Hash.Target......: 35a9c2444ec63ee39f3b214edb9011f32e624a28
Time.Started.....: Fri Oct 16 18:46:37 2020 (20 secs)
Time.Estimated...: Fri Oct 16 18:46:57 2020 (0 secs)
Guess.Mask.......: ?1?1?1?1?1?1?1 [7]
Guess.Charset....: -1 rafelhidgosc?d, -2 Undefined, -3 Undefined, -4
Undefined
Guess.Queue......: 7/8 (87.50%)
Speed.#1.........: 125.5 MH/s (15.03ms) @ Accel:8 Loops:512 Thr:64 Vec:1
Recovered........: 1/1 (100.00%) Digests
Progress.........: 2461270016/2494357888 (98.67%)
Rejected.........: 0/2461270016 (0.00%)
Restore.Point....: 229376/234256 (97.92%)
Restore.Sub.#1...: Salt:0 Amplifier:4096-4608 Iteration:0-512
Candidates.#1....: 0slr5sf -> hcs47o5
Hardware.Mon.#1..: Util:65536% Core: 200MHz Mem:1200MHz Bus:16
```

*Consola 2: Output del programa Hashcat*

## Valoración de las Contraseñas

Una vez obtenidas las contraseñas, podemos observar que todas incumplen la Política de Seguridad de Contraseñas, procederemos a analizarlas una a una.

### Contraseña de jmquevedo, qwerty

Esta incumple tres de los cuatro requisitos, ya que las mayúsculas no se consideran uno, faltando los caracteres numéricos y simbólicos, además de no ser de 8 caracteres. Es un simple recorrido de teclado, son contraseñas vagas y sin ninguna seguridad, ya que todos los diccionarios incluyen estos recorridos en las distintas distribuciones de teclado. Un recorrido de teclado es un tipo de tecleo que consiste en arrastrar el dedo sin levantar de un sitio del teclado a otro.

### Contraseña de mjimenven, vituperio

A pesar de parecer una contraseña más segura que la anterior, se trata simplemente de una palabra del diccionario español, por tanto su nivel de seguridad es muy bajo, incumple dos de los cuatro requisitos, fallando de nuevo en los caracteres numéricos y simbólicos.

### Contraseña de rhgasca, aaeiao5

Aun habiendo hecho falta un ataque por fuerza, se trata de una contraseña con una seguridad muy baja, debido a su longitud, si hubiera sido mas larga podría haber dado más problemas, sin embargo, sigue sin cumplir la Política de Seguridad de Contraseña, no respetando la longitud mínima y faltando un carácter simbólico.

Al tener algo de información sobre la composición de la contraseña, como que era una combinación de letras del nombre y apellidos del usuario y un número, hemos podido acotar la búsqueda del algoritmo y obtener la contraseña usando fuerza bruta. Sin embargo, hemos podido comprobar que estos datos son mentira, ya que la contraseña no ha resultado ser como el usuario decía.

CONFIDENC

Hoy en día, se pueden encontrar múltiples formas de solventar los problemas de las contraseñas débiles, este es el caso de uso de los generadores de contraseñas, se trata de una herramienta sencilla que genera mediante unas especificaciones una amalgama de caracteres para generar la contraseña, debido a su aleatoriedad generan buenas contraseñas, e implementarlas es sencillo, sin embargo debido a su aleatoriedad hace que una contraseña no sea fácilmente memorizable por tanto mucha gente acaba haciendo un uso inadecuado ya que lo apuntan la contraseña en un lugar, en un post-it en la pantalla, o incluso en un archivo de texto plano en el escritorio.

Por tanto, debemos introducir el término de gestores o baúles de contraseñas, que almacenan las contraseñas anteriormente descritas y su nombres de usuario, además de la aplicación web a la que pertenece. Esto resuelve los problemas de memorización que someten a los usuarios, pero genera un punto único de fallo donde el usuario debe ser consciente que esa única contraseña es la llave maestra a toda su información.

Entre los generadores más buscados en la red tenemos,

### ClaveSegura

ClaveSegura, la más simple de las que se describen, se trata de una web que te permite escoger, de forma limitada, los caracteres disponibles y de un tamaño entre 4 y 20 caracteres.

### Strong Password Generator

Strong Password Generator, un poco más completo, añadiendo un recordatorio de como generar una buena contraseña y ampliando el tamaño de la contraseña a 32 caracteres.

### Password Generator

Password Generator es una aplicación web donde nos encontramos la más completa de todas las descritas, incluyendo opciones como no utilizar caracteres ambiguos o similares e incluso generando la contraseña en nuestro ordenador, además de incrementar el número de caracteres hasta 2048.

y a continuación, de los gestores más buscados en la web,

### Exploradores de Internet

Google siendo uno de los gigantes tecnológicos, se metió de lleno en el gestión de contraseñas, integrándolas en todos sus dispositivos, Android, ChromeOS. Pero aún siendo uno de los más usados, ya que viene por defecto en muchos dispositivos, su capacidad de personalización es muy baja.

Apple también cuenta con su gestor, al igual que Google se integra en todos sus dispositivos por defecto e incluye más personalización pudiendo definir más parámetros como caracteres a usar, fácil de leer y longitud entre otras.

Firefox como otro de los exploradores, también tiene integrado en su sistema de cuentas un gestor de contraseñas, sin embargo, también carece de la falta de personalización en la creación de contraseñas.

Pronto se unirá Edge con su generador y gestor propio, que ya se está gestando en las versiones de desarrollo.

CONFIDENCIAL

LastPass ofrece los muchos más servicios que los exploradores anteriores, incluso para un uso personal y gratuito, sin embargo también hay soluciones para empresas que agilizan los procesos de inicio de sesión y creación de contraseñas para los empleados aumentando la productividad y unificando las responsabilidades de la seguridad de la empresa.

Además, por el momento aún no ha habido brechas de seguridad públicas, haciendo que sea una de las mejores opciones a considerar.

### Dashlane

Dashlane incluye más servicios, sin embargo a mayor precio, depende de la empresa habría que hacer un análisis de costes para saber si los servicios que incluyen consiguen igualar o mejorar los resultados de otros gestores. Pudiéndose medir en la capacidad de respuesta, opinión de los usuarios y aumento de la productividad.

## Informe Final

A través de las actividades realizadas anteriormente, hemos llegado a las siguientes conclusiones.

En primer lugar, la empresa debe de tener un sistema de verificación de los parámetros exigidos por la Política de Seguridad de Contraseñas a la hora de introducirlas, esto se puede hacer fácilmente a través de una comprobación en PhP por ejemplo, ver Anexo III, donde se restrinjan las contraseñas no adecuadas.

Sin embargo, también vemos imprescindible la realización de un curso/taller para la concienciación de los trabajadores en el aspecto de seguridad, ya que un sistema es tan seguro como su eslabón más débil, que en la mayoría de los casos se trata del factor humano.

En cuanto a la gestión de las contraseñas, recomendamos tanto Dashlane como LastPass, siendo este último una mejor opción para introducir, ya que su plan gratuito puede servir de toma de contacto para observar si mejora la seguridad y la productividad y una vez refutado el sistema, empezar a plantear las opciones de pago para empresas que incluyen herramientas más avanzadas.

Finalmente, debemos recomendar otras tecnologías para la encriptación de los datos, ya que se han conseguido encontrar colisiones con SHA-1, Shattered, por tanto se han de considerar otras opciones más actuales, por ejemplo haciendo uso de SHA-256 donde se aumenta significativamente el número de bits disminuyendo la posibilidad de colisión, o haciendo uso de un salt combinado con el actual SHA-1, como contraparte, esto conllevaría a una revisión completa de todas las contraseñas de la empresa, decisiones donde la empresa debe asumir los riesgos si el coste de las pérdidas es mayor que los costes de implementación del nuevo sistema, además de los daños en la fiabilidad de la empresa.

CONFIDENCIAL

# Anexo I: Especificaciones técnicas de los recursos

En este anexo, se procederá a exponer los distintos benchmarks realizados con los recursos tecnológicos disponibles, para distintas operaciones de encriptación.

- Ordenador 1, mediante "john --test" en Manjaro KDE 20.1.1

```
Benchmarking: Raw-MD5 [MD5 128/128 AVX 4x3]... DONE
Raw:   41225K c/s real, 41225K c/s virtual

Benchmarking: Raw-SHA1 [SHA1 128/128 AVX 4x]... DONE
Raw:   21896K c/s real, 21896K c/s virtual

Benchmarking: Raw-SHA256 [SHA256 128/128 AVX 4x]... (4xOMP) DONE
Raw:   30605K c/s real, 7807K c/s virtual

Benchmarking: Raw-SHA512 [SHA512 128/128 AVX 2x]... (4xOMP) DONE
Raw:   13826K c/s real, 3473K c/s virtual
```

- HP Pavilion x360, mediante "hashcat64.exe -b" en Windows 10

```
Hashmode: 0 - MD5
Speed.#1.........:  2192.4 MH/s (88.56ms) @ Accel:64 Loops:1024 Thr:1024 Vec:8

Hashmode: 100 - SHA1
Speed.#1.........:   772.1 MH/s (64.86ms) @ Accel:32 Loops:512 Thr:1024 Vec:1

Hashmode: 1400 - SHA2-256
Speed.#1.........:   275.4 MH/s (91.03ms) @ Accel:8 Loops:1024 Thr:1024 Vec:1

Hashmode: 1700 - SHA2-512
Speed.#1.........: 77053.0 kH/s (81.30ms) @ Accel:2 Loops:1024 Thr:1024 Vec:1
```

- ASUSPRO P2520LA, mediante "hashcat64.exe -b" en Windows 10

```
Hashmode: 0 - MD5
Speed.#1.........:  1736 MH/s (37.45ms) @ Accel:256 Loops:1024 Thr:64 Vec:1

Hashmode: 100 - SHA1
Speed.#1.........:  1042.0 MH/s (49.05ms) @ Accel:128 Loops:1024 Thr:64 Vec:1

Hashmode: 1400 - SHA2-256
Speed.#1.........:   382.0 MH/s (63.42ms) @ Accel:512 Loops:128 Thr:64 Vec:1

Hashmode: 1700 - SHA2-512
Speed.#1.........: 75964.2 kH/s (71.28ms) @ Accel:16 Loops:1024 Thr:64 Vec:1
```

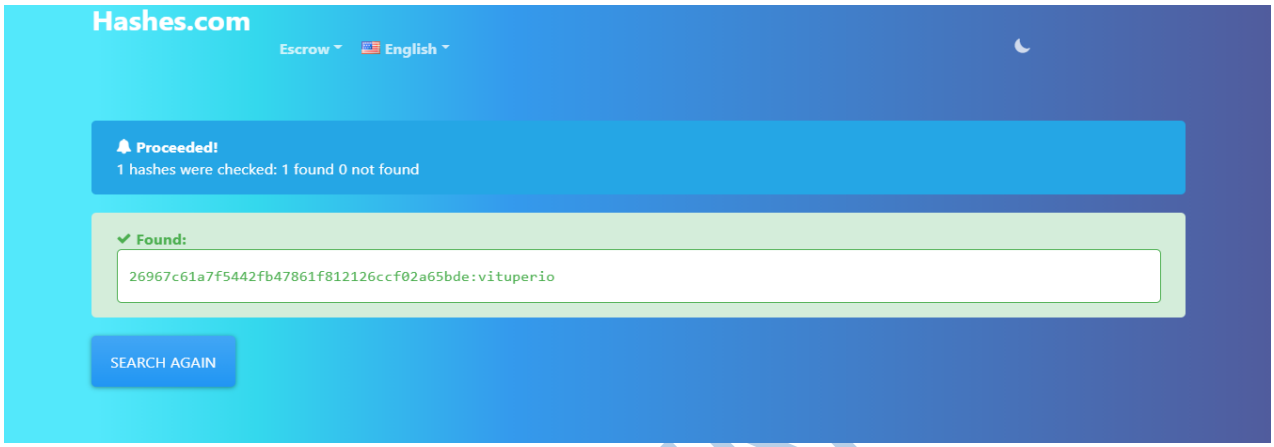
- HUAWEI MateBook D 14 AMD, mediante "hashcat64.exe -b" en Windows 10

```
Hashmode: 0 - MD5
Speed.#1.........:  2672.5 MH/s (48.82ms) @ Accel:256 Loops:1024 Thr:64 Vec:1

Hashmode: 100 - SHA1
Speed.#1.........:  1030.4 MH/s (63.54ms) @ Accel:128 Loops:1024 Thr:64 Vec:1

Hashmode: 1400 - SHA2-256
Speed.#1.........:   425.0 MH/s (77.50ms) @ Accel:512 Loops:128 Thr:64 Vec:1

Hashmode: 1700 - SHA2-512
Speed.#1.........: 95363.9 kH/s (86.34ms) @ Accel:16 Loops:1024 Thr:64 Vec:1
```

Estos resultados nos indican que la máquina más potente es el HUAWEI MateBook D 14 AMD, con una velocidad para calcular hashes por fuerza bruta de 1030 millones de hashes por segundo, es decir, aproximadamente 2  hashes por segundo, un número que puede parecer grande hasta que lanzamos el número posible de combinaciones que se obtendrían con los parámetros mínimos con 2  aproximadamente, haciendo que el tiempo necesario para calcular todos los hashes sea de 35 días.

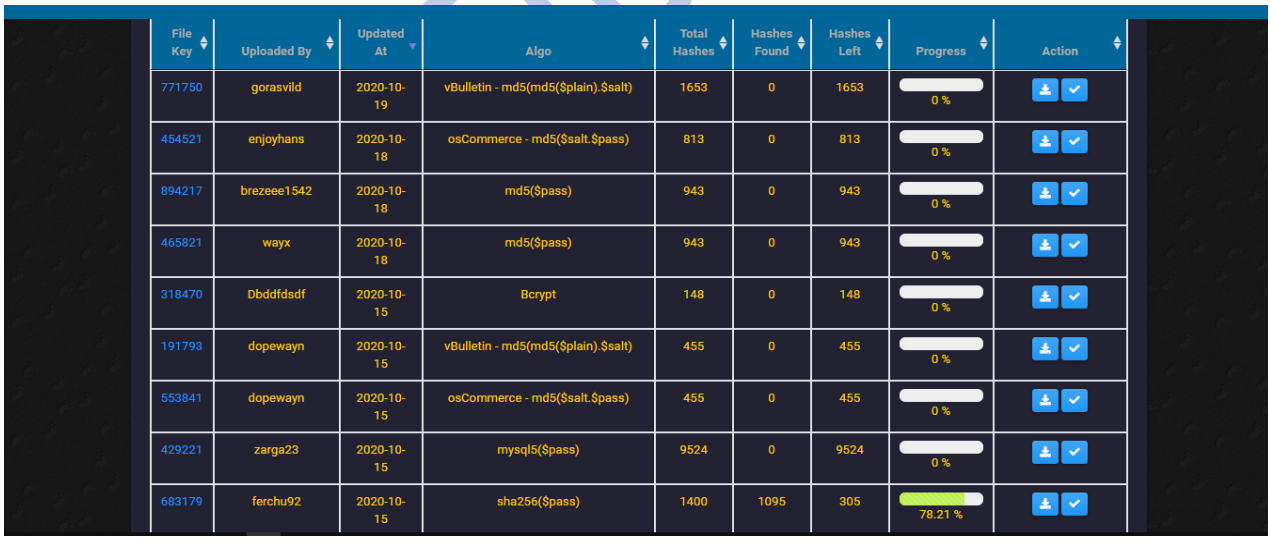
# Anexo II: Uso de las Aplicaciones Web para la consulta de hashes

En este anexo, se detalla una guía de uso general de una aplicación web para la consulta de hashes comunes, en este caso se ha usado Hashes.com, donde simplemente al acceder, nos aparece un cuadro de búsqueda y solo tenemos que introducir el hash deseado, si se encuentra entre los más populares seguramente se consiga obtener el origen del mismo.




Estas webs se caracterizan por tener listas de contraseñas filtradas a través de un fallo de seguridad, como el sucedido con RockYou.

En algunos casos, recuerdan que los datos introducidos en ningún momento son privados, que incluso para romper esos hashes se envían a equipos de otros usuarios para que presten su hardware y puedan solucionar esa tarea y por eso se asume que todo el contenido que se envía es legal.



| File Key | Uploaded By | Updated At | Algo | Total Hashes | Hashes Found | Hashes Left | Progress | Action |
|---|---|---|---|---|---|---|---|---|
| 771750 | gorasvild | 2020-10-19 | vBulletin - md5(md5($plain).$salt) | 1653 | 0 | 1653 | 0 % | |
| 454521 | enjoyhans | 2020-10-18 | osCommerce - md5($salt.$pass) | 813 | 0 | 813 | 0 % | |
| 894217 | brezeee1542 | 2020-10-18 | md5($pass) | 943 | 0 | 943 | 0 % | |
| 465821 | wayx | 2020-10-18 | md5($pass) | 943 | 0 | 943 | 0 % | |
| 318470 | Dbddfdsdf | 2020-10-15 | Bcrypt | 148 | 0 | 148 | 0 % | |
| 191793 | dopewayn | 2020-10-15 | vBulletin - md5(md5($plain).$salt) | 455 | 0 | 455 | 0 % | |
| 553841 | dopewayn | 2020-10-15 | osCommerce - md5($salt.$pass) | 455 | 0 | 455 | 0 % | |
| 429221 | zarga23 | 2020-10-15 | mysql5($pass) | 9524 | 0 | 9524 | 0 % | |
| 683179 | ferchu92 | 2020-10-15 | sha256($pass) | 1400 | 1095 | 305 | 78.21 % | |

Como vemos en la imagen anterior, en estas mismas paginas también tienes la posibilidad de descargarte los hashes que se van generando de los archivos que los usuarios han subido y ver el tipo en el que se ha generado.

# Anexo III: Función en PhP para la Comprobación de Contraseñas

A continuación, se expondrá un fragmento de código que comprueba que las contraseñas cumplen con los parámetros de seguridad acordados por la empresa.

```
function validar_clave($contrasena,&$error_contrasena){
   if(strlen($contrasena) < 6){
      $error_contrasena = "La contraseña debe tener al menos 6 caracteres";
      return false;
   }
   if (!preg_match(``[a-z]``,$contrasena)){
      $error_contrasena = "La contraseña debe tener al menos una letra
minúscula";
      return false;
   }
   if (!preg_match(``[A-Z]``,$contrasena)){
      $error_contrasena = "La contraseña debe tener al menos una letra
mayúscula";
      return false;
   }
   if (!preg_match(``[0-9]``,$contrasena)){
      $error_contrasena = "La contraseña debe tener al menos un caracter
numérico";
      return false;
   }
   if (!preg_match(``\x{0021}-\x{002F}\x{003A}-\x{0040}\x{005B}-\x{005F}\
x{007B}-\x{007D}``,$contrasena)){
      $error_contrasena = "La contraseña debe tener al menos uno de los
siguientes caracteres simbólicos";
      return false;
   }
   $error_contrasena = "";
   return true;
}
```

CONF