

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



Escuela Técnica Superior de  
**Ingeniería Informática**

# Índice

Alcance y Objetivos de la Auditoría.....	3
Estudio Inicial.....	3
Estudio de las Tecnologías Adecuadas y Alternativas.....	3
<b>Tabla Arcoiris.....</b>	<b>3</b>
<b>Ataque de Diccionario.....</b>	<b>3</b>
<b>Fuerza Bruta.....</b>	<b>4</b>
Recursos para la Auditoría.....	4
Recursos Humanos.....	4
Recursos Tecnológicos.....	4
Actividades de la Auditoría.....	5
Análisis de Hashes.....	5
<b>Ataque de Diccionario.....</b>	<b>5</b>
<b>Ataque por Fuerza Bruta.....</b>	<b>5</b>
Valoración de las Contraseñas.....	6
<b>Contraseña de jmquevedo, qwerty.....</b>	<b>6</b>
<b>Contraseña de mjimenven, vituperio.....</b>	<b>6</b>
<b>Contraseña de rhgasca, aaeiao5.....</b>	<b>6</b>
Análisis de Generadores y Gestores de Contraseñas.....	7
<b>ClaveSegura.....</b>	<b>7</b>
<b>Strong Password Generator.....</b>	<b>7</b>
<b>Password Generator.....</b>	<b>7</b>
<b>Exploradores de Internet.....</b>	<b>7</b>
<b>LastPass.....</b>	<b>8</b>
<b>Dashlane.....</b>	<b>8</b>
Informe Final.....	8
Anexo I: Especificaciones técnicas de los recursos.....	9
Anexo II: Uso de las Aplicaciones Web para la consulta de hashes.....	10

## 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 la siguiente tabla:

Nombre del Usuario	Username	Hash de la Contraseña
Manuel Jimen Ventoyk	mjimenv	26967c61a7f5442fb47861f812126ccf02a65bde
José María Quevedo Yuw	jmquevedo	b1b3773a05c0ed0176787a4f1574ff0075f7521eHash de la Contraseña 26967c61a7f5442fb47861f812126ccf02a65bde b1b3773a05c0ed0176787a4f1574ff0075f7521e 35a9c2444ec63ee39f3b214edb901f32e624a28
Rafael Hidalgo Gasca	rhtagasca	35a9c2444ec63ee39f3b214edb901f32e624a28

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 Arcoiris

Una tabla arcoiris 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 ataques 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, además para este hay multitud de opciones online, por ejemplo, [Hashes.com](https://hashes.com), [md5decrypt.net](https://md5decrypt.net), o algunos con más opciones como [dcode.fr](https://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](https://github.com/MatthewJohnRipper/John-the-Ripper) para Linux o [Hash Suite](https://www.ginsim.com/hash-suite/) y [Hashcat](https://github.com/hashcat/hashcat) para Windows, usando un diccionario adecuado siendo entre los más populares [RockYou](https://rockyou.com) y un diccionario reciente como [Koanashi](https://koanashi.com).

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 crearla, 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 descryptado 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

- HUAWEI MateBook D 14 AMD,
  - AMD Ryzen 5 3500U
  - Radeon™ Vega 8 Graphics
  - 8 GB DDR4
  - 512 GB PCIe SSD

## Actividades de la Auditoría

Las distintas actividades que se realizarán 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 Hash Suite. Para ello se utilizaron distintos 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, 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
- -l 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.

```
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 [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.

## Análisis de Generadores y Gestores de Contraseñas

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.

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

Integer vitae lacus consequat, semper lorem at, feugiat purus. In fermentum eget mauris iaculis malesuada. Maecenas egestas enim nec nisl ullamcorper aliquam. Pellentesque tempus dictum ipsum, eget bibendum purus pretium id. Sed mattis magna dapibus erat bibendum facilisis. Ut pulvinar lectus volutpat posuere aliquet. Aliquam a ligula placerat, fermentum mauris non, iaculis dolor. Vestibulum a dolor sapien. Ut vitae dolor et tortor fermentum imperdiet. Aliquam sodales molestie viverra. Suspendisse aliquet nulla a nunc ornare dignissim.

CONFIDENTIAL



## Anexo I: Especificaciones técnicas de los recursos

CONFIDENCIAL

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

CONFIDENCIAL